DATA PROTECTION LAWS OF THE WORLD

Full Handbook

Downloaded: 10 October 2024

TABLE OF CONTENTS

Albania 24
Algeria 33
Angola 39
Argentina 44
Armenia 48
Aruba 55
Australia 60
Austria 68
Azerbaijan 82
Bahamas 84
Bahrain 88
Bangladesh 93
Barbados 96
Belarus 100
Belgium 107
Benin 123
Bermuda 130
Bolivia 133
Bonaire, Sint Eustatius and Saba 136
Bosnia and Herzegovina 141
Botswana 147
Brazil 155
British Virgin Islands 165
Brunei 170
Bulgaria 175
Burkina Faso 191
Burundi 197
Cambodia 200
Canada 206
Cape Verde 215
Cayman Islands 219
Chad 226
Chile 232
China 238
Colombia 250
Costa Rica 259
Croatia 263
Cuba 275
Curaçao 278
Cyprus 283
Czech Republic 297
Democratic Republic of Congo 308
Denmark 312
Dominican Republic 331
Ecuador 335
Egypt 343
El Salvador 349
Equatorial Guinea 352
Estonia 355
Ethiopia 370

Federated States of Micronesia . . . 373
Fiji . . . 375
Finland . . . 378
France . . . 392
Gabon . . . 410
Georgia . . . 418
Germany . . . 422
Ghana . . . 439
Gibraltar . . . 447
Greece . . . 460
Guatemala . . . 478
Guernsey . . . 481
Guinea . . . 498
Haiti . . . 502
Honduras . . . 505
Hong Kong, SAR . . . 509
Hungary . . . 516
Iceland . . . 527
India . . . 541
Indonesia . . . 553
Iran . . . 564
Ireland . . . 568
Israel . . . 585
Italy . . . 595
Japan . . . 609
Jersey . . . 616
Jordan . . . 628
Kazakhstan . . . 634
Kenya . . . 640
Kosovo . . . 648
Kuwait . . . 657
Kyrgyzstan . . . 660
Laos . . . 665
Latvia . . . 670
Lebanon . . . 683
Lesotho . . . 686
Liberia . . . 691
Libya . . . 695
Lithuania . . . 700
Luxembourg . . . 714
Macau . . . 728
Madagascar . . . 731
Malaysia . . . 735
Malta . . . 741
Mauritius . . . 757
Mexico . . . 764
Moldova . . . 772
Monaco . . . 777
Mongolia . . . 783
Montenegro . . . 790
Morocco . . . 795
Mozambique . . . 799

Myanmar . . . 803
Namibia . . . 805
Nepal . . . 807
Netherlands . . . 811
New Zealand . . . 825
Nicaragua . . . 834
Niger . . . 837
Nigeria . . . 843
North Macedonia . . . 852
Norway . . . 859
Pakistan . . . 873
Panama . . . 878
Paraguay . . . 883
Peru . . . 888
Philippines . . . 896
Poland . . . 905
Portugal . . . 919
Qatar . . . 933
Qatar - Financial Centre . . . 938
Republic of Congo . . . 944
Romania . . . 947
Russia . . . 962
Rwanda . . . 969
Saudi Arabia . . . 975
Senegal . . . 978
Serbia . . . 984
Seychelles . . . 990
Singapore . . . 995
Sint Maarten . . . 1002
Slovak Republic . . . 1007
Slovenia . . . 1022
South Africa . . . 1036
South Korea . . . 1042
Spain . . . 1049
Sri Lanka . . . 1063
Sweden . . . 1072
Switzerland . . . 1085
Taiwan . . . 1094
Tajikistan . . . 1099
Tanzania . . . 1102
Thailand . . . 1109
Tonga . . . 1115
Trinidad and Tobago . . . 1117
Tunisia . . . 1121
Turkey . . . 1126
Turkmenistan . . . 1135
UAE - Abu Dhabi Global Market Free Zone . . . 1138
UAE - Dubai (DIFC) . . . 1147
UAE - Dubai Health Care City Free Zone . . . 1156
UAE - General . . . 1161
Uganda . . . 1174
Ukraine . . . 1178

United Kingdom 1185
United States 1198
Uruguay 1210
Uzbekistan 1214
Venezuela 1221
Vietnam 1225
Zambia 1237
Zimbabwe 1242

I. INTRODUCTION

EU data protection legislation is facing huge changes. Data protection laws are built on fundamental rights enshrined in the Charter of Fundamental Rights of the European Union which are the core building blocks of the EU’s legal regime. Privacy issues arising from an exponential growth in consumer and mobile technologies, an increasingly connected planet and mass cross-border data flows have pushed the EU to entirely rethink its data protection legislation to ensure that these fundamental rights are fully protected in today’s digital economy.

In 2012, the European Commission published a draft regulation (the General Data Protection Regulation, 'GDPR'). Just over four years later, the final text of GDPR was published in the Official Journal of the European Union on April 27, 2016. Regulation 2016/679 heralds some of the most stringent data protection laws in the world and has been in force since May 25, 2018.

The previous EU Data Protection Directive (95/46/EC) was adopted in 1995. It was implemented differently by EU Member States into their respective national jurisdictions, resulting in the fragmentation of national data protection laws within the EU. As it is a Regulation, GDPR came into effect immediately on May 25, 2018 without any need for additional domestic legislation in EU Member States. However, with more than 30 areas where Member States are permitted to legislate (differently) in their domestic laws there will continue to be significant variation in both substantive and procedural data protection laws among the EU’s different Member States.

With fines of up to 4% of total worldwide annual turnover for failing to comply with the requirements of GDPR, organizations have had a great deal to do to comply with the new regime.

II. CURRENT SITUATION

After almost four years of often fractious negotiations, GDPR was published in the Official Journal of the European Union as Regulation 2016/679 on April 27, 2016.

There was a two-year transition period to allow organizations and governments to adjust to the new requirements and procedures. Following the end of this transitional period, the Regulation became directly applicable throughout the EU from May 25, 2018, without requiring implementation by the EU Member States through national law.

The goal of European legislators was to harmonize the previous legal framework, which was fragmented across Member States. A 'Regulation' (unlike a Directive) is directly applicable and has consistent effect in all Member States, and GDPR was intended to increase legal certainty, reduce the administrative burden and cost of compliance for organizations that are active in multiple EU Member States, and enhance consumer confidence in the single digital marketplace. However, in order to reach political agreement on the final text there are more than 30 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws. There continues to be room for different interpretation and enforcement practices among the Member States. There is therefore likely to continue to be significant differences in both substantive and procedural data protection laws and enforcement practice among EU Member States with GDPR in force.

We have summarized the key changes introduced by the GDPR in the following sections.

Key changes to the previous data protection framework include:

A. WIDER TERRITORIAL SCOPE

Where organizations are established within the EU

GDPR applies to processing of personal data “in the context of the activities of an establishment” (Article 3(1)) of any organization within the EU. For these purposes “establishment” implies the “effective and real exercise of activity through stable arrangements” (Recital 22) and “the legal form of such arrangements…is not the determining factor” (Recital 22), so there is a wide spectrum of what might be caught from fully functioning subsidiary undertakings on the one hand, to potentially a single individual sales representative depending on the circumstances.

Europe’s highest court, the Court of Justice of the European Union (the CJEU) has been developing jurisprudence on this concept, recently finding (*Google Spain SL, Google Inc. v AEPD*, *Mario Costeja Gonzalez* (C-131/12)) that Google Inc. with EU-based sales and advertising operations (in that particular case, a Spanish subsidiary) was established within the EU. More recently, the same court concluded (*Weltimmo v NAIH* (C-230/14)) that a Slovakian property website was also established in Hungary and therefore subject to Hungarian data protection laws.

Where organizations are not established within the EU

Even if an organization is able to prove that it is not established within the EU, it will still be caught by GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "to the offering of goods or services" (Art 3(2)(a)) (no payment is required) to such data subjects in the EU or "the monitoring of their behavior" (Art 3(2)(b)) as far as their behavior takes place within the EU. Internet use profiling (Recital 24) is expressly referred to as an example of monitoring.

Practical implications

1. Compared to the previous Directive, GDPR captures many more overseas organizations. US tech should particularly take note as the provisions of GDPR have clearly been designed to capture them.

2. Overseas organizations not established within the EU who are nevertheless caught by one or both of the offering goods or services or monitoring tests must designate a representative within the EU (Article 27).

B. TOUGHER SANCTIONS

Revenue-based fines

GDPR joins anti-bribery and anti-trust laws as having some of the very highest sanctions for non-compliance including revenue-based fines of up to 4% of annual worldwide turnover.

To compound the risk for multinational businesses, fines are imposed by reference to the revenues of an undertaking rather than the revenues of the relevant controller or processor. Recital 150 of GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully the Treaty doesn’t define the term either and the extensive case-law is not entirely straightforward with decisions often turning on the specific facts of each case. However, in many cases group companies have been regarded as part of the same undertaking. This is bad news for multinational businesses as it means that in many cases group revenues will be taken into account when calculating fines, even where some of those group companies have nothing to do with the processing of data to which the fine relates provided they are deemed to be part of the same undertaking. The assessment will turn on the facts of each case.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to 20,000,000 Euros or in the case of an undertaking up to 4% of total worldwide turnover of the preceding year, whichever is higher apply to breach of:

- the basic principles for processing including conditions for consent
- data subjects’ rights
- international transfer restrictions
- any obligations imposed by Member State law for special cases such as processing employee data
- certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to 10,000,000 Euros or in the case of an undertaking up to 2% of total worldwide turnover of the preceding year, whichever is the higher apply to breach of:

- obligations of controllers and processors, including security and data breach notification obligations
- obligations of certification bodies

- obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Broad investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

GDPR makes it considerably easier for individuals to bring private claims against data controllers and processors. In particular:

- any person who has suffered "material or non-material damage" as a result of a breach of GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress and hurt feelings even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80). Although this falls someway short of a US style class action right, it certainly increases the risk of group privacy claims against consumer businesses. Employee group actions are also more likely under GDPR.

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Practical implications

1. The scale of fines and risk of follow-on private claims under GDPR means that actual compliance is a must. GDPR is not a legal and compliance challenge – it is much broader than that, requiring organizations to completely transform the way that they collect, process, securely store, share and securely wipe personal data. Engagement of senior management and forming the right team is key to successful GDPR readiness.

2. Organizations caught by GDPR need to map current data collection and use, carry out a gap analysis of their current compliance against GDPR and then create and implement a remediation plan, prioritizing high risk areas.

3. GDPR requires suppliers and customers to review supply chains and current contracts. Contracts will need to be renegotiated to ensure GDPR compliance and commercial terms will inevitably have to be revisited in many cases given the increased costs of compliance and higher risks of non-compliance.

4. The very broad concept of 'undertaking' is likely to put group revenues at risk when fines are calculated, whether or not all group companies are caught by GDPR or were responsible for the infringement of its requirements. Multinationals even with quite limited operations caught by GDPR will therefore need to carefully consider their exposure and ensure compliance.

5. Insurance arrangements need to be reviewed and cyber and data protection exposure added to existing policies or purchased as stand-alone policies where possible. The terms of policies require careful review as there is wide variation among wordings and many policies may not be suitable for the types of losses which are likely to occur under GDPR.

C. MORE DATA CAUGHT

Personal data is defined as "any information relating to an identified or identifiable natural person.” (Article 4) A low bar is set for "identifiable" – if anyone can identify a natural person using “all means reasonably likely to be used”

(Recital 26) the information is personal data, so data may be personal data even if the organization holding the data cannot itself identify a natural person. A name is not necessary either – any identifier will do such as an identification number, location data, an online identifier or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30 with IP addresses, cookies and RFID tags all listed as examples.

Although the definition and recitals are broader than the equivalent definitions in the current Directive, for the most part they are simply codifying current guidance and case law on the meaning of 'personal data'.

GDPR also includes a broader definition of "special categories" (Article 9) of personal data which are more commonly known as sensitive personal data. The concept has been expanded to expressly include the processing of genetic data and biometric data. The processing of these data are subject to a much more restrictive regime.

A new concept of 'pseudonymisation' (Article 4) is defined as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Organizations which implement pseudonymization techniques enjoy various benefits under GDPR.

Practical implications

1. If in any doubt, it is prudent to work on the assumption that data is personal data given the extremely wide definition of personal data in GDPR.

2. GDPR imposes such a high bar for compliance, with sanctions to match, that often the most effective approach to minimize exposure is not to process personal data in the first place and to securely wipe legacy personal data or render it fully anonymous, reducing the amount of data subject to the requirements of GDPR.

3. Where a degree of identification is required for a specific purpose, the next best option is only to collect and use pseudonymous data. Although this falls within the regulated perimeter, it enjoys a number of benefits for organizations in particular that in the event of a data breach it is much less likely that pseudonymous data will cause harm to the affected individuals, thereby also reducing the risk of sanctions and claims for the relevant organization.

4. Organizations should only use identifiable personal data as a last resort where anonymous or pseudonymous data is not sufficient for the specific purpose.

D. SUPPLIERS (PROCESSORS) CAUGHT TOO

GDPR directly regulates data processors for the first time. The current Directive generally regulates controllers (i.e., those responsible for determining the purposes and means of the processing of personal data) rather than 'data processors' - organizations who may be engaged by a controller to process personal data on their behalf (e.g., as an agent or supplier).

Under GDPR, processors are required to comply with a number of specific obligations, including to maintain adequate documentation (Article 30), implement appropriate security standards (Article 32), carry out routine data protection impact assessments (Article 32), appoint a data protection officer (Article 37), comply with rules on international data transfers (Chapter V) and cooperate with national supervisory authorities (Article 31). These are in addition to the requirement for controllers to ensure that when appointing a processor, a written data processing agreement is put in place meeting the requirements of GDPR (Article 28). Again, these requirements have been enhanced and gold-plated compared to the equivalent requirements in the Directive.

Processors are directly liable to sanctions (Article 83) if they fail to meet these criteria and may also face private claims by individuals for compensation (Article 79).

Practical implications

1. GDPR completely changes the risk profile for suppliers processing personal data on behalf of their customers. Suppliers now face the threat of revenue-based fines and private claims by individuals for failing to comply with GDPR. Telling an investigating supervisory authority that you are just a processor won’t work; they can fine you too. Suppliers need to take responsibility for compliance and assess their own compliance with GDPR. In many cases, this requires the review and overhaul of current contracting arrangements to ensure better compliance. The increased compliance burden and risk requires a careful review of business cases.

2. Suppliers need to decide for each type of processing undertaken whether they are acting solely as a processor or if their processing crosses the line and renders them a data controller or joint controller, attracting the full burden of GDPR.

3. Customers (as controllers) face similar challenges. Supply chains need to be reviewed and assessed to determine current compliance with GDPR. Privacy impact assessments need to be carried out. Supervisory authorities may need to be consulted. In many cases contracts are likely to need to be overhauled to meet the new requirements of GDPR. These negotiations will not be straightforward given the increased risk and compliance burden for suppliers. They will also be time consuming and it would be sensible to start the renegotiation exercise sooner rather than later, particularly as suppliers are likely to take a more inflexible view over time as standard positions are developed.

4. There are opportunities for suppliers to offer GDPR “compliance as a service” solutions, such as secure cloud solutions, though customers will need to review these carefully to ensure they dovetail to their own compliance strategy.

E. DATA PROTECTION PRINCIPLES

The core themes of the data protection principles in GDPR remain largely as they were in the Directive, though there has been a significant raising of the bar for lawful processing (see Higher Bar for Lawful Processing) and a new principle of accountability has been added.

Personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle")
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle")
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle")
- accurate and where necessary kept up-to-date (the "accuracy principle")
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle")
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle")

The controller is responsible for and must be able to demonstrate compliance with the above principles (the accountability principle).

Practical implications

1. Controllers need to assess and ensure compliance of data collection and use across their organizations with each of the above principles as any failure to do so attracts the maximum category of fines of up to 20 million Euros / 4% of worldwide annual turnovers. Data mapping, gap analysis and remediation action plans need to be undertaken and implemented.

2. The enhanced focus on accountability will require a great deal more papering of process flows, privacy controls and decisions made to allow controllers to be able to demonstrate compliance. See Accountability and Governance

F. HIGHER BAR FOR LAWFUL PROCESSING

The lawfulness, fairness and transparency principle among other things requires processing to fall within one or more of the permitted legal justifications for processing. Where special categories of personal data are concerned, additional much more restrictive legal justifications must also be met.

Although this structure is present in the Directive, the changes introduced by GDPR will make it much harder for organizations to fall within the legal justifications for processing. Failure to comply with this principle is subject to the very highest fines of up to 20 million Euros or in the case of an undertaking up to 4% of annual worldwide turnover, whichever is the greater.

In particular:

- The bar for valid consents has been raised much higher under GDPR. Consents must be fully unbundled from other terms and conditions and will not be valid unless freely given, specific, informed and unambiguous (Articles 4(11) and 6(1)(a)). Consent also attracts additional baggage for controllers in the form of extra rights for data subjects (the right to be forgotten and the right to data portability) relative to some of the other legal justifications. Consent must be as easy to withdraw consent as it is to give – data subjects have the right to withdraw consent at any time – and unless the controller has another legal justification for processing any processing based on consent alone would need to cease once consent is withdrawn.
- To compound the challenge for controllers, in addition to a hardening of the requirements for valid consent, GDPR has also narrowed the legal justification allowing data controllers to process in their legitimate interests. This justification also appears in the Directive though the interpretation of the concept in the current regime has varied significantly among the different Member States with some such as the UK and Ireland taking a very broad view of the justification and others such as Germany taking a much more restrictive interpretation. GDPR has followed a more Germanic approach, narrowing the circumstances in which processing will be considered to be necessary for the purposes of the legitimate interests of the controller or a third party. In particular, the ground can no longer be relied upon by public authorities. Where it is relied upon, controllers will need to specify what the legitimate interests are in information notices and will need to consider and document why they consider that their legitimate interests are not overridden by the interests or fundamental rights and freedoms of the data subjects, in particular where children’s data is concerned.

The good news is that the justification allowing processing necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject to enter into a contract is preserved in GDPR, though continues to be narrowly drafted. Processing which is not necessary to the performance of a contract will not be covered. The less good news for controllers relying on this justification is that it comes with additional burdens under GDPR, including the right to data portability and the right to be forgotten (unless the controller is able to rely on another justification).

Other justifications include where processing is necessary for compliance with a legal obligation; where processing is necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent; where processing is necessary for performance of a task carried out in the public interest in the exercise of official authority vested in the controller. These broadly mirror justifications in the previous Directive.

Processing for new purposes

It is often the case that organizations will want to process data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data was first collected. This is potentially in conflict with the core principle of purpose limitation and to ensure that the rights of data subjects are protected, GDPR sets out a series of considerations that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are a fresh consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Processing of special categories of personal data

As is the case in the Directive, GDPR sets a higher bar to justify the processing of special categories of personal data. These are defined to include "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation." (Article 9(1)) Processing of these data are prohibited unless one or more specified grounds are met which are broadly similar to the grounds set out in the Directive.

Processing of special categories of personal data is only permitted (Article 9(2)):

- with the explicit consent of the data subject
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- in limited circumstances by certain not-for-profit bodies
- where processing relates to the personal data which are manifestly made public by the data subject
- where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

The justifications and conditions for processing special categories of data is one area where Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Processing of personal data relating to criminal convictions and offenses

GDPR largely mirrors the requirements of the Directive in relation to criminal conviction and offences data. This data may only be processed under official authority or when authorized by Union or Member State law (Article 10) which means this is another area where legal requirements and practice is likely to diverge among the different Member States.

Practical Implications

1. Controllers need to ensure that they have one or more legal justifications to process personal data for each purpose. Practically this will require comprehensive data mapping to ensure that all personal data within the extended enterprise (i.e. including data processed by third parties as well as data within the organization) has a legal justification to be processed.

2. Consideration needs to be given as to which are the most appropriate justifications for different purposes and personal data, given that some justifications attract additional regulatory burdens.

3. The common practice of justifying processing with generic consents needs to cease with GDPR in force. Consent comes with many additional requirements under GDPR and as such is likely to be a justification of last resort where no other justifications are available.

4. Where controllers propose to process legacy data for new purposes, they need to be able to demonstrate compliance with the purpose limitation principle. To do that, controllers should document decisions made concerning new processing, taking into

account the criteria set out in GDPR and bearing in mind that technical measures such as encryption or psuedonymisation of data will generally make it easier to prove that new purposes are compatible with the purposes for which personal data were originally collected.

G. TRANSFERS

International transfers and particularly those to the US have regularly made front page headline news over the last 12 months with the successful torpedoing of the EU/US Safe Harbor regime by Europe's highest court. Organizations will be relieved to hear that for the most part GDPR does not make any material changes to the previous rules for transfers of personal data cross-border, largely reflecting the regime under the Directive. That said, in contrast to the previous regime where sanctions for breaching transfer restrictions are limited, failure to comply with GDPR's transfer requirements attract the highest category of fines of up to 20 million Euros or in the case of undertakings up to 4% of annual worldwide turnover.

Transfers of personal data to third countries outside the EU are only permitted where the conditions laid down in GDPR are met (Article 44).

Transfers to third countries, territories or specified sectors or an international organization which the Commission has decided ensures an adequate level of protection do not require any specific authorization (Article 45(1)). The adequacy decisions made under the current Directive shall remain in force under GDPR until amended or repealed (Article 45(9)); so for the time being transfers to any of the following countries are permitted: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

The well-publicized gap for transfers from the EU to US following the ruling that Safe Harbor is invalid will, it is hoped, be filled with the new EU/US Privacy Shield.

Transfers are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards include among other things binding corporate rules which now enjoy their own Article 47 under GDPR and standard contractual clauses. Again, decisions on adequacy made under the Directive will generally be valid under GDPR until amended, replaced or repealed.

Two new mechanics are introduced by GDPR to justify international transfers (Article 46(2)(e) and (f)): controllers or processors may also rely on an approved code of conduct pursuant to Article 40 or an approved certification mechanism pursuant to Article 42 together in each case with binding and enforceable commitments in the third country to apply these safeguards including as regards data subjects' rights. GDPR also removes the need to notify and in some Member States seek prior approval of model clauses from supervisory authorities.

GDPR includes a list of derogations similar to those included in the Directive permitting transfers where:

(a) explicit informed consent has been obtained
(b) the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
(d) the transfer is necessary for important reasons of public interest
(e) the transfer is necessary for the establishment, exercise or defense of legal claims
(f) the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
(g) the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanic is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48)are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in

force between the requesting third country and the EU or Member State; otherwise transfer in response to such requests where there is no other legal basis for transfer will breach GDPR's restrictions.

Practical Implications

1. Given the continued focus of the media and regulators on international transfer and the increased sanctions to be introduced by GDPR, all controllers and processors need to carefully diligence current data flows to establish what types of data is being shared with which organizations in which jurisdictions.

2. Current transfer mechanics need to be reviewed to assess compliance with GDPR and, where necessary, remedial steps implemented before GDPR comes into force.

3. For intra-group transfers, consider binding corporate rules which not only provide a good basis for transfers but also help demonstrate broader compliance with GDPR helping to comply with the principle of accountability.

H. DATA BREACH NOTIFICATION

One of the most profound changes to be introduced by GDPR is a European wide requirement to notify data breaches to supervisory authorities and affected individuals.

In the US, data breach notification laws are now in force in all 50 States and the hefty penalties for failing to notify have fundamentally changed the way US organizations investigate and respond to data incidents. Not notifying has become a high risk option.

In contrast, Europe previously had no universally applicable law requiring notification of breaches. In the majority of Member States there was either no general obligation to notify or minimal sanctions for failing to do so; for many organizations not notifying and thereby avoiding the often damaging media fall-out is still common practice in Europe. That fundamentally changes with GDPR in force.

GDPR requires "the controller without undue delay, and where feasible, not later than 72 hours after having become aware of it, [to] notify the … breach to the supervisory authority" (Article 33(1)). When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals the controller is also required to notify the affected individuals "without undue delay" (Article 34). Processors are required to notify the controller without undue delay having become aware of the breach (Article 33(2)).

The notification to the regulator must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s DPO or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Although the obligation to notify is conditional on awareness, burying your head in the sand is not an option as controllers are required to implement appropriate technical and organizational measures together with a process for regularly testing, assessing and evaluating the effectiveness of those measures to ensure the security of processing (Article 32). Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits by the supervisory authority.

Failing to comply with the articles relating to security and data breach notification attract fines of up to 10 million Euros or 2% of annual worldwide turnover, potentially for both the controller and the processor. As data breach often leads to investigations by supervisory authorities and often uncovers other areas of non-compliance, it is quite possible that fines of up to 20 million Euros or 4% of annual worldwide turnover will also be triggered.

Practical implications

1. Notification will become the norm: Sweeping breaches under the carpet has become a very high risk option under GDPR. Organizations that are found to have deliberately not notified can expect the highest fines and lasting damage to corporate and individual reputations. Notifying and building data breach infrastructure to enable prompt, compliant notification will be a necessity under GDPR.

2. A coordinated approach, including technology, breach response policy and training and wider staff training. Data breaches are increasingly a business as usual event. Lost or stolen devices; emails sent to incorrect addresses in error and the continuing rise of cybercrime means that for many organizations, data breaches are a daily occurrence. To deal with the volume of breaches, organization's need a combination of technology, breach response procedures and staff training.

a. Technology requirements: these will vary for each organization but will typically include a combination of firewalls, log recording, data loss prevention, malware detection and similar applications. There are an increasingly sophisticated array of applications that learn what “normal” looks like for a particular corporate network to be able to spot unusual events more effectively. The state of the art continues to change rapidly as organizations try to keep pace with sophisticated hackers. Regular privacy impact assessments and upgrades of technology are required.
b. Breach response procedures: to gain the greatest protection from technology, investment is required in dealing with red flags when they are raised by internal detection systems or notified from external sources. Effective breach response requires a combination of skill sets including IT, PR and legal. Develop a plan and test it regularly.
c. Staff training: the weak link in security is frequently people rather than technology. Regular staff training is essential to raise awareness of the importance of good security practices, current threats and who to call if a breach is suspected. It is also important to avoid a blame culture that may deter staff from reporting breaches.

3. Consider privilege and confidentiality as part of your plan. Make sure that forensic reports are protected by privilege wherever possible to avoid compounding the losses arising from a breach. Avoid the temptation to fire off emails when a breach is suspected; pick up the phone. Don’t speculate on what might have happened; stick to the facts. Bear in mind that you may be dealing with insider threat – such as a rogue employee – so keep any investigation on a strictly need to know basis and always consider using external investigators if there is any possibility of an inside attack.

4. Appoint your external advisors today if you haven’t done so already. When a major incident occurs, precious time can be wasted identifying and then retaining external support teams when you are up against a 72 hour notification deadline. Lawyers, forensics and PR advisors should ideally be contracted well before they are needed for a live incident. Find out more about DLA Piper's breach response credentials and team.

5. Insurance: many insurers are now offering cyber insurance. However, there is a lack of standardization in coverage offered. Limits are often too small for the likely exposure. Conditions are often inappropriate such as a requirement for the insured to have fully complied with all applicable laws and its own internal policies which will rarely be the case. That said, it is usually possible to negotiate better coverage with carriers in what continues to be a soft insurance market. Now is a good time to check the terms of policies and work with your legal team and brokers to ensure that you have the best possible coverage. You should clarify with brokers and underwriters what amounts to a notifiable incident to insurers under your policies as again there is no common standard and failing to notify when required may invalidate cover. You should also ensure that your insurance policies will cover the costs of your preferred external advisors as many policies will only cover advice from panel advisors.

6. Develop standard notification procedures: Perhaps the greatest challenge facing organizations and regulators is the sheer volume of data breach and the lack of standards or guidance as to how breaches should be notified and at what point they become notifiable. In the absence of guidance organization's will need to make an informed decision as to how to develop internal operations for the detection, categorization, investigation, containment and reporting of data breaches. Similarly, supervisory authorities will need to develop standard approaches and standard categorizations of incidents to ensure that limited resources are focused on the most serious incidents first.

I. MORE RIGHTS FOR INDIVIDUALS

GDPR builds on the rights enjoyed by individuals under the previous Directive, enhancing those rights and introducing a new right to data portability. These rights are backed up with provisions making it easier to claim damages for compensation and for consumer groups to enforce rights on behalf of consumers.

Transparency

One of the core building blocks of GDPR’s enhanced rights for individuals is the requirement for greater transparency. Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data is obtained:

- the identity and contact details of the controller
- the Data Protection Officer's contact details (if there is one)
- both the purpose for which data will be processed and the legal basis for processing including if relevant the legitimate interests for processing
- the recipients or categories of recipients of the personal data
- details of international transfers
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- the existence of rights of the data subject including the right to access, rectify, require erasure (the “right to be forgotten”), restrict processing, object to processing and data portability; where applicable the right to withdraw consent, and the right to complain to supervisory authorities
- the consequences of failing to provide data necessary to enter into a contract
- the existence of any automated decision making and profiling and the consequences for the data subject.
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Slightly different transparency requirements apply (Article 14) where information have not been obtained from the data subject.

Subject access rights (Article 15)

These broadly follow the existing regime set out in the Directive though some additional information must be disclosed and there is no longer a right for controllers to charge a fee, with some narrow exceptions. Information requested by data subjects must be provided within one month as a default with a limited right for the controller to extend this period for up to three months.

Right to rectify (Article 16)

Data subjects continue to enjoy a right to require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure (right to be forgotten)(Article 17)

This forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right to be forgotten now has its own Article in GDPR. However, the right is not absolute; it only arises in quite a narrow set of circumstances notably where the controller has no legal ground for processing the information. As demonstrated in the Google Spain decision itself, requiring a search engine to remove search results does not mean the underlying content controlled by third party websites will necessarily be removed. In many cases the controllers of those third party websites may have entirely legitimate grounds to continue to process that information, albeit that the information is less likely to be found if links are removed from search engine results.

The practical impact of this decision has been a huge number of requests made to search engines for search results to be removed raising concerns that the right is being used to remove information that it is in the public interest to be accessible.

Right to restriction of processing (Article 18)

Data subjects enjoys a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data is no longer needed save for legal claims of

the data subject, or where the legitimate grounds for processing by the controller and whether these override those of the data subject are contested.

Right to data portability (Article 20)

This is an entirely new right in GDPR and has no equivalent in the previous Directive. Where the processing of personal data is justified either on the basis that the data subject has given their consent to processing or where processing is necessary for the performance of a contract, or where the processing is carried out be automated means, then the data subject has the right to receive or have transmitted to another controller all personal data concerning them in a structured, commonly used and machine-readable format.

The right is a good example of the regulatory downsides of relying on consent or performance of a contract to justify processing – they come with various baggage under GDPR relative to other justifications for processing.

Where the right is likely to arise controllers need to develop procedures to facilitate the collection and transfer of personal data when requested to do so by data subjects.

Right to object (Article 21)

The Directive's right to object to the processing of personal data for direct marketing purposes at any time is retained.

In addition, data subjects have the right to object to processing which is legitimized on the grounds either of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject or that the processing is for the establishment, exercise or defense of legal claims.

The right not to be subject to automated decision making, including profiling (Article 22)

This right expands the Directive right not to be subject to automated decision making. GDPR expressly refers to profiling as an example of automated decision making. Automated decision making and profiling "which produces legal effects concerning [the data subject] … or similarly significantly affects him or her" are only permitted where

(a) necessary for entering into or performing a contract
(b) authorized by EU or Member State law, or
(c) the data subject has given their explicit (i.e. opt-in) consent.

The scope of this right is potentially extremely broad and may throw into question legitimate profiling for example to detect fraud and cybercrime. It also presents challenges for the online advertising industry and website operators who will need to revisit consenting mechanics to justify online profiling for behavioral advertising. This is an area where further guidance is needed on how Article 22 will be applied to specific types of profiling.

Practical implications

1. Controllers need to review and update current fair collection notices to ensure compliance with the expanded information requirements. Much more granular notices are required using plain and concise language.

2. Consideration should be given to which legal justifications for processing are most appropriate for different purposes, given that some such as consent and processing for performance of a contract come with additional regulatory burden in the form of enhanced rights for individuals.

3. For some controllers with extensive personal data held on consumers, it is likely that significant investment in customer preference centers is required on the one hand to address enhanced transparency and choice requirements and on the other hand to automate compliance with data subject rights.

4. Existing data subject access procedures should be reviewed to ensure compliance with the additional requirements of GDPR.

5. Policies and procedures need to be written and tested to ensure that controllers are able to comply with data subjects’ rights within the time limits set by GDPR. In some cases, such as where data portability engages, significant investments may be required.

J. DATA PROTECTION OFFICERS

GDPR introduces a significant new governance burden for those organizations which are caught by the new requirement to appoint a DPO. Although this was already a requirement for most controllers in Germany under previous data protection laws, it is an entirely new requirement (and cost) for many organizations.

The following organizations must appoint a data protection officer (DPO) (Article 37):

- public authorities
- controllers or processors whose core activities consist of processing operations which by virtue of their nature, scope or purposes require regular and systemic monitoring of data subjects on a large scale
- controllers or processors whose core activities consist of processing sensitive personal data on a large scale.

DPOs must have "expert knowledge" (Article 37(5)) of data protection law and practices though perhaps in recognition of the current shortage of experienced data protection professionals, it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "properly and in a timely manner in all issues which relate to the protection of personal data" (Article 38(1)). The role is therefore a sizeable responsibility for larger controllers and processors.

The DPO must directly report to the highest management level, must not be told what to do in the exercise of their tasks and must not be dismissed or penalized for performing their tasks (Article 38(3)).

The specific tasks of the DPO are set out in GDPR including (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws
- to monitor compliance with law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- to advise and monitor data protection impact assessments
- to cooperate and act as point of contact with the supervisory authority

Practical implications

1. Organizations need to assess whether or not they fall within one or more of the categories where a DPO is mandated. Public authorities will be caught (with some narrow exceptions) as will many social media, search and other tech firms who monitor online consumer behavior to serve targeting advertising. Many b2c businesses which regularly monitor online activity of their customers and website visitors will also be caught.

2. There is currently a shortage of expert data protection officers as outside of Germany this is a new requirement for most organizations. Organizations will therefore need to decide whether to appoint an internal DPO with a view to training them up over the next couple of years or use one of the external DPO service providers several of which have been established to fill this gap in the market. Organizations might consider a combination of internal and external DPO resources as given the size of the task it may not be realistic for just one person to do it.

K. ACCOUNTABILITY AND GOVERNANCE

Accountability is a recurring theme of GDPR. Data governance is no longer just a case of doing the right thing; organizations need to be able to prove that they have done the right thing to regulators, to data subjects and potentially to shareholders and the media often years after a decision was taken.

GDPR requires each controller to demonstrate compliance with the data protection principles (Article 5(2)). This general principle manifests itself in specific enhanced governance obligations which include:

- ***Keeping a detailed record of processing operations*** (Article 30)
  The requirement in previous data protection laws to notify the national data protection authority about data processing operations was abolished and replaced by a more general obligation on the controller to keep extensive internal records of their data protection activities. The level of detail required is far more granular compared to many previous Member State notification requirements. There is some relief granted to organizations employing fewer than 250 people though the exemption is very narrowly drafted.
- ***Performing data protection impact assessment for high risk processing*** (Article 35)
  A data protection impact assessment is a mandatory pre-requisite before processing personal data for processing which is likely to result in a high risk to the rights and freedoms of individuals. Specific examples are set out of high risk processing requiring impact assessments including: automated processing including profiling that produce legal effects or similarly significantly affect individuals; processing of sensitive personal data; and systematic monitoring of publicly accessible areas on a large scale. DPOs, where in place, have to be consulted. Where the impact assessment indicates high risks in the absence of measures to be taken by the controller to mitigate the risk, the supervisory authority must also be consulted (Article 36) and may second guess the measures proposed by the controller and has the power to require the controller to impose different or additional measures (Article 58).
- ***Designating a data protection officer*** (Article 37) See Data Protection Officers
- ***Notifying and keeping a comprehensive record of data breaches*** (Articles 33 and 34) See Data Breach Notification
- ***Implementing data protection by design and by default*** (Article 25)
  GDPR introduces the concepts of "data protection by design and by default." "Data protection by design" requires taking data protection risks into account throughout the process of designing a new process, product or service, rather than treating it as an afterthought. This means assessing carefully and implementing appropriate technical and organizational measures and procedures from the outset to ensure that processing complies with GDPR and protects the rights of the data subjects.
  "Data protection by default" requires ensuring mechanisms are in place within the organization to ensure that, by default, only personal data which are necessary for each specific purpose are processed. This obligation includes ensuring that only the minimum amount of personal data is collected and processed for a specific purpose; the extent of processing is limited to that necessary for each purpose; the data is stored no longer than necessary and access is restricted to that necessary for each purpose.

Practical implications

1. Data mapping: every controller and processor needs to carry out an extensive data audit across the organization and supply chains, record this information in accordance with the requirements of Article 30 and have governance in place to ensure that the information is kept up-to-date. The data mapping exercise is also be crucial to be able to determine compliance with GDPR’s other obligations so this exercise should be commenced as soon as possible.

2. Gap analysis: Once the data mapping exercise is complete, each organization needs to assess its current level of compliance with the requirements of GDPR. Gaps need to be identified and remedial actions prioritized and implemented.

3. Governance and policy for data protection impact assessments: the data mapping exercise should identify high risk processing. Data protection impact assessments need to be completed and documented for each of these (frequently these will include third party suppliers) and any remedial actions identified implemented. Supervisory authorities may need to be consulted. A procedure needs to be put in place to standardize future data protection impact assessments and to keep existing impact assessments regularly updated where there is a change in the risk of processing.

4. Data protection by design and by default: in part these obligations will be addressed through implementing remedial steps identified by the gap analysis and in data protection impact assessments. However, to ensure that data protection by design and by default is delivered, extensive staff and supplier engagement and training will also be required to raise awareness of the importance of data protection and to change behaviors.

L. DEROGATIONS

European data protection laws today are in many cases substantively very different among Member States. This is partly due to the ambiguities in the Directive being interpreted and implemented differently, and partly due to the Directive permitting Member States to implement different or additional rules in some areas. As GDPR will become law without the need for any secondary implementing laws, there will be a greater degree of harmonization relative to the current regime. However, GDPR preserves the right for Member States to introduce different laws in many important areas and as a result we are likely to continue to see a patchwork of different data protection laws among Member States, for certain types of processing.

Each Member State is permitted to restrict the rights of individuals and transparency obligations (Article 23) by legislation when the restriction "respects the essence of fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society" to safeguard one of the following:

(a) national security
(b) defense
(c) public security
(d) the prevention, investigation, detection or prosecution of breaches of ethics for regulated professions, or crime, or the execution of criminal penalties
(e) other important objectives of general public interest of the EU or a Member State, in particular economic or financial interests
(f) the protection of judicial independence and judicial proceedings
(g) a monitoring, inspection or regulatory function connected with national security, defense, public security, crime prevention, other public interest or breach of ethics
(h) the protection of the data subject or the rights and freedoms of others
(i) the enforcement of civil law claims

To be a valid restriction for the purposes of GDPR, any legislative restriction must contain specific provisions setting out:

(a) the purposes of processing
(b) the categories of personal data
(c) the scope of the restrictions
(d) the safeguards to prevent abuse or unlawful access or transfer
(e) the controllers who may rely on the restriction
(f) the permitted retention periods
(g) the risks to the rights and freedoms of data subjects
(h) the right of data subjects to be informed about the restriction, unless prejudicial to the purpose of the restriction

In addition to these permitted restrictions, Chapter IX of GDPR sets out various specific processing activities which include additional derogations, exemptions and powers for Member States to impose additional requirements. These include:

- processing and freedom of expression and information (Article 85)
- processing and public access to official documents (Article 86)
- processing of national identification numbers (Article 87)
- processing in the context of employment (Article 88)
- safeguards and derogations to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 89)
- obligations of secrecy (Article 90)
- existing data protection rules of churches and religious associations (Article 91)

These special cases also appeared in the Directive, though in some cases have been amended or varied in GDPR.

Practical implications

1. Controllers and processors first need to determine which Member States' laws apply to their processing activities and whether processing will be undertaken within any specific processing activities which may be subject to additional restrictions.

2. These Member State laws then need to be checked to determine what additional requirements engage. Changes in law need to be monitored and any implications for processing activities addressed.

3. Derogations pose a challenge to multi-national organizations seeking to implement standard European-wide solutions to address compliance with GDPR; these need to be sufficiently flexible to allow for exceptions where different rules engage in one or more Member State.

M. CROSS-BORDER ENFORCEMENT

The ideal of a one-stop-shop ensuring that controllers present in multiple Member States would only have to answer to their lead home regulator failed to make it into the final draft. GDPR includes a complex, bureaucratic procedure allowing multiple 'concerned' authorities to input into the decision making process.

The starting point for enforcement of GDPR is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities and there are powers for a supervisory authorities in another Member State to enforce where infringements occur on its territory or substantially affects data subjects only in its territory (Article 56(2)).

In situations where multiple supervisory authorities are involved in an investigation or enforcement process there is a cooperation procedure (Article 60) involving a lengthy decision making process and a right to refer to the consistency mechanism (Articles 63 - 65) if a decision cannot be reached, ultimately with the European Data Protection Board having the power to take a binding decision.

There is an urgency procedure (Article 66) for exceptional circumstances which permits a supervisory authority to adopt provisional measures on an interim basis where necessary to protect the rights and freedoms of data subjects.

Practical implications

1. Controllers and processors need to determine which Member States' supervisory authorities have jurisdiction over their processing activities; which is the lead authority and which other supervisory authorities may have jurisdiction.

2. An important aspect of managing compliance risk is to try to stay on the right side of your regulator by engaging positively with any guidance published and taking up opportunities such as training and attending seminars.

DATA PROTECTION AND PRIVACY GROUP KEY CONTACTS

Americas

Jennifer Kashatus
Partner
T +1 202 799 4448
jennifer.kashatus@dlapiper.com

Kate Lucente
Partner and Co-Editor, Data Protection Laws of the World
T +1 813 222 5927
kate.lucente@dlapiper.com

Andrew Serwin
Partner, Global Co-Chair Data Protection, Privacy and Security Group
T +1 858 677 1418
andrew.serwin@dlapiper.com

Europe, Middle East and Africa

Andrew Dyson
Partner, Global Co-Chair Data Protection, Privacy and Security Group
T +44 (0)113 369 2403
andrew.dyson@dlapiper.com

Ewa Kurowska-Tober
Partner, Global Co-Chair Data Protection, Privacy and Security Group
T +48 22 540 74 1502
ewa.kurowska-tober@dlapiper.com

Denise Lebeau-Marianna
Partner
T + 33 (0)1 40 15 24 98
denise.lebeau-marianna@dlapiper.com

Diego Ramos
Partner
T +349 17901658
diego.ramos@dlapiper.com

Richard van Schaik
Partner
T +31 20 541 9828
richard.vanschaik@dlapiper.com

Asia Pacific

Carolyn Bigg

Nicholas Boyle
Partner

Partner, Global Co-Chair of Data Protection, Privacy and Security Group
T +852 2103 0576
carolyn.bigg@dlapiper.com

T +61 2 9286 8479
nicholas.boyle@dlapiper.com

EDITORS

James Clark
Partner
T +44 113 369 2461
james.clark@dlapiper.com

Kate Lucente
Partner and Co-Editor, Data Protection Laws of the World
T +1 813 222 5927
kate.lucente@dlapiper.com

Lea Lurquin
Associate and Contributing Editor, Data Protection Laws of the World
T +1 415 615 6024
lea.lurquin@dlapiper.com

ALBANIA

Last modified 27 December 2022

LAW

The Republic of Albania regulates personal data protection pursuant to Law No. 9887, dated 10 March 2008 "On Protection of Personal Data", as amended ("**Data Protection Law**") (Official Gazette of the Republic of Albania No. 44, dated 1 April 2008). The Data Protection Law was last amended in 2014, thus it is yet to be harmonized with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**").

The complete harmonization of the current Albanian legislation in force on data protection with the GDPR has been one of the main objectives of the Office of Information and Data Protection Commissioner since 2018, however this objective has yet to be achieved (due in part to the Covid-19 pandemic).

In June 2022 the Ministry of Justice of the Republic of Albania launched a public consultation process on a draft law “On Personal Data Protection” which is approximated with the GDPR. As of December 2022 this draft law has yet to be approved by the Albanian Parliament.

Earlier in the year, on 28 January 2022, Albania signed the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which was later ratified by Law No. 49/2022, dated 12 May 2022 “ *On the Ratification of the Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*”.

DEFINITIONS

Definition of Personal Data

Data Protection Law defines personal data as any information relating to an identified or identifiable natural person, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Definition of Sensitive Personal Data

Data Protection Law defines sensitive data as any information related to a natural person referring to his racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, criminal prosecution, as well as data concerning his health and sexual life.

NATIONAL DATA PROTECTION AUTHORITY

The Right to Information and Data Protection Commissioner (the "**Commissioner**") is the Albanian independent authority in charge of supervising and monitoring the protection of personal data and the right to information by respecting and guaranteeing the fundamental human rights and freedoms in compliance with the legal framework.

The Commissioner is a public legal person, elected by the Parliament upon a proposal of the Council of Ministers for a 5-year term, eligible for re-election. The Parliament also designates the organizational structure of the Commissioner’s Office.

The information obtained by the Commissioner while exercising his duties shall be used only for supervisory purposes in compliance with the legislation on the protection of personal data. The Commissioner shall remain under the obligation of confidentiality even after the termination of his functions.

The Commissioner is seated at Rr. "Abdi Toptani", Nd. 5, 1001, Tirana, Albania.

REGISTRATION

Data Protection Law provides for the legal obligation of every controller to notify the Commissioner on the processing of personal data for which it is responsible. The notification shall be made before the controller processes the data for the first time, or when a change of the processing notification status is required.

The notification shall contain the name and address of the controller, the purpose of personal data processing, the categories of data subjects and personal data, the recipients and categories of the recipients of personal data, the proposal on the international transfers that the controller aims to carry out and a general description of the measures for the security of personal data. The notification is done either online, on the website of the Commissioner, or manually, by submitting the completed notification form to the Commissioner's Office.

The information submitted by the data controller through the notification, except for the general description of the measures for the security of personal data, shall be published by the Commissioner’s Office on the Electronic Register of Controllers which is accessible by the public on the official website.

The notification process and the publication of the information it contains is fundamental to ensure transparency for the public and consequently to protect personal data. Through the access to the Electronic Register of Controllers, the public has the means of understanding how personal data are processed by the controlling entities.

The failure of the controlling entities to comply with the obligation to notify the Commissioner constitutes an administrative offence and is punishable by a fine.

However, there are cases when the controllers are exempted from the notification obligation as follows:

- The processing of personal data is performed in order to keep a register, which in accordance with the law or sub-legal acts provides information for the public;
- The processing of personal data is performed in order to protect the constitutional institutions, national security interests, foreign policies, economic or financial interests of the state, or for the prevention or prosecution of criminal offences;
- The processing of data is done pursuant to Decision of the Commissioner No. 4 "On the Determination of the Cases Exempted from the Notification Obligation of the Personal Data which are Processed", dated 27 December 2012.

DATA PROTECTION OFFICERS

In compliance with the responsibility to issue instructions on measures to be undertaken for the activity of specific sectors, the Commissioner has issued two instructions:

- Instruction No. 22 "On the Determination of Rules for Maintaining the Security of Personal Data Processed by Small Processing Entities", dated 24 September 2012, as amended.

Small processing entities shall mean the controllers or processors that process personal data by way of electronic or manual means, by fewer than six processing persons, either directly or through processors.

- Instruction No. 47 "On the Determination of Rules for Maintaining the Security of Personal Data Processed by Large Processing Entities", dated 14 September 2018.

Large processing entities shall mean the controllers or processors that process personal data by way of electronic or manual means, by six or more processing persons, either directly or through processors.

Personal data processing entities are responsible for the internal supervision of the protection of the processed personal data. Each subject that is subject to instruction no. 47, dated 14 September 2018 (i.e., large processing entities), shall authorize in writing at least one Data Protection Officer ("**DPO**") *(Albanian terminology: Contact Person)* who shall be charged to carry out the internal supervision. Small processors contracted by large processors are also advised to appoint a DPO.

Instruction no. 47, dated 14 September 2018 determines the criteria that a person must fulfil in order to be appointed as a DPO, as well as the duties and responsibilities of a DPO, which include, among others:

- the internal supervision of the fulfilment of the obligations for the protection of personal data by the personal data processing entity;
- the implementation of technical, organizational and staff related measures;
- the necessary cooperation with the Commissioner;
- etc.

COLLECTION & PROCESSING

Data Protection Law states that fair and lawful processing is one of the core principles for the protection of personal data. Personal data shall be collected and/or processed for specific, clearly defined and legitimate purposes.

Personal data protection is based on data adequacy, data which are relevant to the purpose of their processing and not excessive in relation to such purpose, as well as data accuracy, data which are updated and complete.

Additionally, the data are to be kept in a form that allows the identification of data subjects for no longer than it is necessary for the purpose for which they were collected or further processed.

Data Protection Law provides for the legal criteria for personal data processing, sensitive data processing and special processing of data.

Personal data may be processed only:

- with the consent of the personal data subject;
- if necessary, for the performance of a contract to which the data subject is a party or in order to negotiate or amend a draft/contract at the request of the data subject;
- to protect the vital interests of the data subject;
- to comply with a legal obligation of the controller;
- for the performance of a legal task of public interest or in exercise of powers of the controller or of a third party to whom the data are disclosed;
- if the processing is necessary for the protection of the legitimate rights and interests of the controller, the recipient or any other interested party. However, in any case, the processing of personal data cannot be in clear contradiction with the data subject's right to protection of personal life and privacy.

The processing of personal data in the field of national security, criminal law and crime prevention, shall be performed by official authorities as stipulated in the law.

The controller or processor that processes personal data for the purpose of offering business opportunities or services may use personal data obtained from a public data list. The controller or processor cannot process these data further, if the data subject has expressed his disagreement or has objected their further processing.

It should be noted that additional personal data cannot be added to the data obtained from the public data list without the consent of the data subject. However, the controller is allowed to keep these personal data in its filing system even after the data subject has objected the processing. Such data can be used only if the data subject gives his content.

Collection of personal data which is related to a data subject solely for reasons of direct marketing is allowed only if the data subject has given his explicit consent.

Sensitive data may be processed only if:

- the data subject has given his consent, which may be revoked at any given moment making any further processing of data illegal;
- it is in the vital interest of the data subject or another person and the data subject is physically or mentally incapable of giving his consent;
- it is authorized by the responsible authority for an important public interest, under adequate safeguards;
- it is related to data which are widely made known by the data subject or it is necessary, for exercising/protecting a legal right;
- the data are processed for historic, scientific or statistical purposes, under adequate safeguards;
- the data are required for the purposes of preventive medicine, medical diagnosis, the provision of health care, treatment or management of health care services and the data are used by the medical personnel or other persons with the obligation to preserve confidentiality;
- the data are processed by non-profit political, philosophical or religious organizations and trade unions for purposes of their legitimate activity, only for members, sponsors, or other persons related to their activity. These data shall not be disclosed to a third party without the consent of the data subject unless otherwise stipulated by law.
- the data processing is necessary for the purpose of fulfilling the legal obligations and specific rights of the controller in the field of employment in compliance with the Labour Code.

Special processing of data:

- Processing for historical, scientific and statistical purposes:

Personal data collected for any purpose, may be further processed for historic, scientific or statistical purposes, provided that the data is not processed in order to take measures or decisions related to an individual.

The transmission of sensitive data for scientific research shall take place only in case of an important public interest. Personal data shall be used exclusively by individuals who are bound by the obligation of confidentiality. When data processing is made in a manner that allows the identification of the data subject, the data should be encrypted immediately in order for the subjects to be no longer identifiable. Encrypted personal data shall be used exclusively by individuals bound by the obligation of confidentiality.

- Processing of personal data and freedom of expression:

The Commissioner has issued an Instruction No. 31, dated 27 December 2012 "On the Determination of the Conditions and Criteria for the Exemption from the relevant Obligations in Personal Data Processing for Journalism, Literature or Artistic Purposes". The exemptions for these purposes shall be allowed up to the extent that they reconcile the right of personal data protection with the rules governing the right to freedom of expression.

TRANSFER

The international transfer of personal data may be carried out with recipients from states which have an adequate level of personal data protection. The level of personal data protection for a state is established by assessing all circumstances related to the nature, purpose and duration of the processing, the country of origin and final destination, as well as the legal provisions and security standards in force in the recipient state.

Pursuant to the Decision of the Commissioner No. 8, dated 31 October 2016 the following states have an adequate level of data protection:

- European Union member states;
- European Economic Area states;
- Parties to the Convention No. 108 of the Council of Europe "For the Protection of Individuals with regard to Automatic Processing of Personal Data", as well as its 1981 Protocol, which have approved a special law and set up a supervisory authority that operates in complete independence, providing appropriate legal mechanisms, including handling complaints, investigating and ensuring the transparency of personal data processing;
- States where personal data may be transferred, pursuant to a decision of the European Commission.

International transfer of personal data with a state that does not have an adequate level of personal data protection may be done if:

- it is authorized by international acts ratified by the Republic of Albania which are directly applicable;
- the data subject has given his consent for the international transfer;
- the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken in addressing a request of the data subject, or the transfer is necessary for the conclusion or performance of a contract between the controller and a third party, in the interest of the data subject;
- it is a legal obligation of the controller;
- it is necessary for protecting vital interests of the data subject;
- it is necessary or constitutes a legal requirement over an important public interest or for exercising and protecting a legal right;
- it is done from a register that is open for consultation and provides information to the general public.

Pursuant to the Data Protection Law, the Commissioner issues instructions in order to allow certain categories of personal data to be transferred to a state that does not have an adequate level of personal data protection. In these cases, the controller is exempted from the authorization request. Accordingly, the Commissioner has issued the Instruction No. 41, dated 13 June 2014 "On allowing some categories of international transfers of personal data in a country that does not have an adequate level of personal data protection".

Controllers wishing to transfer personal data to other countries lacking adequate personal data protection, may fill in an application form "*For the approval of the transfer of personal data to a state that does not have an adequate level of data protection, through the authorization of the Commissioner*".

In 2014, the Commissioner has also issued a Manual on the International Transfer of Personal Data which provides guidelines to the international transfer of personal data.

The exchange of personal data with the diplomatic representations of foreign governments or international institutions in the Republic of Albania shall be considered an international transfer of data.

SECURITY

Data Protection Law introduces the obligation of the data controller or processor to undertake appropriate organizational and technical measures to protect personal data from unlawful or accidental destruction, accidental loss, or from being accessed or disclosed by unauthorized persons, as well as from any kind of unlawful processing.

The controller is under the obligation to document the measures it has undertaken to ensure protection of personal data, in compliance with the law and other legal regulations.

The data controller undertakes the following special security measures:

- defines the functions among the organizational units and the operators for the use of data;
- the use of data shall be done by order of authorized organizational units or operators;

- instructs all operators on their obligations arising from the data protection legal framework;
- prohibits access of unauthorized persons to the working facilities of the data controller or processor;
- data and programs shall be accessed only by authorized persons;
- prohibits access to and use of the filing system by unauthorized persons;
- data processing equipment shall be operated only with an authorization and every device shall be secured with preventive measures against unauthorized operation;
- records and documents data alteration, rectification, erasure, transfer etc.

The level of security shall be in compliance with the nature of personal data processing. The Commissioner has established the detailed rules for personal data security by means of Decision No. 6, dated 05 August 2013 "On the Determination of Detailed Rules for the Security of Personal Data".

The recorded data may only be used in accordance with their collection purpose, unless they are used to guarantee national security, public security, for the prevention or investigation of a criminal offence, or prosecution of the author thereof, or of any infringement of ethics of the regulated professions.

The data documentation shall be kept for as long as it is necessary for their collection purpose.

The obligation of confidentiality and integrity of the controllers, processors and any other persons that come to know the content of the processed data while exercising their duty shall survive the termination of their functions. The processed data shall not be disclosed unless provided otherwise by law. Anyone acting under the authority of the controller or the processor shall not process the personal data to which they have access, without the authorization of the controller, unless obliged by law.

BREACH NOTIFICATION

Data Protection Law does not provide for a general obligation of the data controller or data processor to notify the Commissioner in case of personal data breach.

However, pursuant to Instruction No. 47, dated 14 September 2018 "On the Determination of Rules for Maintaining the Security of Personal Data Processed by Large Processing Entities", which, as mentioned above applies only to large data processing entities, the DPO shall promptly notify the large data processing entity in writing of any risk of violation of the data subjects' rights, including in case of the violation of personal data protection legislation.

In the event that, following the notification of the DPO, the large data processing entity fails to take appropriate measures to address the problem in a timely manner, the DPO notifies the Commissioner without delay. Therefore, in case of breach of data handled by a large data processing entity, resulting from the violation of violation of the data subjects' rights, or from the violation of personal data protection legislation, which has not been addressed effectively, the DPO has the obligation to notify the Commissioner.

It should also be noted, that pursuant to an opinion of the Commissioner on the protection of personal data on the websites of public and private controllers, data subjects have the right to be notified by the data controller if their personal data have been compromised (data has been lost or stolen, or if their online privacy is likely to be negatively affected). To the best of our understanding the opinion expressed by the Commissioner in this opinion, merely serves as a guideline and has not a binding effect.

On the other hand, Law No. 9918, dated 19 May 2008 "On Electronic Communications in the Republic of Albania", as amended ("**Electronic Communications Law**"), (Official Gazette of the Republic of Albania No. 84, dated 10 June 2008) provides for another breach notification procedure.

The Electronic Communications Law defines personal data breach as *any breach of security leading to the destruction, loss, alteration or unauthorized distribution, accidental or unlawful, or access to personal data transmitted, stored or processed, in connection with the provision of an electronic communications service available to the public.*

Pursuant to article 122 of the Electronic Communications Law, entrepreneurs of public electronic communications networks and services are under the obligation to, individually or when necessary, in cooperation with each-other, implement technical and organizational measures, to ensure the security of networks and/or services, provided by them.

These measures are meant to ensure an adequate level of protection and security of personal data against potential, foreseeable risks. With respect to the personal data of the users, entrepreneurs of public electronic communications networks and services are under the obligation to inform their users about any specific risk, how the risk can be reduced by the users, as well as the possible costs, which must be covered by the user, if the risk that happens is beyond the measures that the entrepreneur can take.

In addition, in case of personal data breach, the entrepreneur who provides electronic communications services available to the public promptly notifies the Authority of Electronic and Postal Communications ("**AEPC**"). When the breach of personal data may adversely affect the personal data and privacy of the subscriber or individual, the entrepreneur shall also promptly notify the said subscriber or individual.

However, if the entrepreneur has proved to the AEPC that it has implemented the necessary technological protection measures and these measures have been applied to the relevant data, then the entrepreneur is not required to notify the subscriber or the individual of the violation of personal data. These technological safeguards ensure that the personal data become illegible to any person who does not have authorized access to the data.

ENFORCEMENT

The Commissioner is the competent authority for the supervision and enforcement of Data Protection Law. The Commissioner has the right to:

- conduct administrative investigations, have access to personal data processing and collect all the necessary information in order to fulfil his supervisory obligations;
- order the blocking, erasure, destruction or suspension of the unlawful processing of personal data;
- give instructions prior to the processing of data and ensure their publication.

In cases of recurring or intentional serious infringement of the Data Protection Law by a controller or processor, the Commissioner acts in compliance with article 39 of Data Protection Law and reports the case publicly or reports it to the Parliament and the Council of Ministers.

Article 39 (1) of Data Protection Law specifies that data processing in violation of the Data Protection Law constitutes administrative offences and may be subject to administrative fines which vary from 10,000 ALL (approx. 83 EUR) to 1,000,000 ALL (approx. 8300 EUR), with legal persons being subject to double the amount specified herein.

Data Protection Law also states that the fine is doubled when the following provisions are breached:

- When the data subject has filed a complaint, the controller shall have no right to make any changes to the personal data until a final decision is reached.
- The Commissioner is responsible for authorizing, in special cases, the use of personal data for purposes not designated during the phase of their collection in compliance with the principles of the Data Protection Law.

The sanctioned subject may appeal the fine in court within the deadlines and according to the procedures that regulate the administrative trials.

Fines shall be paid no later than 30 days from their issuing. When the deadline expires, the decision becomes an executive title and is executed in a mandatory manner by the bailiff's office, upon request of the Commissioner. Fines are cashed in the state budget.

In case the offence consists in a crime, the Commissioner files the relevant criminal charges with the competent law enforcement authorities.

ELECTRONIC MARKETING

Data Protection Law provides that the collection of personal data related to a data subject, solely for reasons of direct marketing is allowed only if the data subject has given his explicit consent.

Data Protection Law defines direct marketing as *the communication of the promotional material, by every means and way, using personal data of legal or natural persons, agencies or other entities with or without interference.*

Moreover, the data subject has the right to demand the controller not to start processing, or in case the processing has started, to stop processing personal data related to him for the purposes of direct marketing and to be informed in advance before personal data are disclosed for the first time for such purpose.

The Commissioner has issued an Instruction no. 06, dated 28 May 2010 "On the correct use of SMSs for promotional purposes, advertising, information, direct sales, via mobile phone". This instruction emphasizes the importance of the prior consent given by the data subject.

In addition, pursuant to article 124 of the Electronic Communications Law, electronic communications service providers may process traffic data for marketing purposes only after prior approval by the subscriber. Subscribers should be informed on the type of traffic data being processed, before give approval for their processing. Subscribers and users have the right to withdraw to any time from the approval they have made.

ONLINE PRIVACY

The Data Protection Law does not provide for regulatory measures targeting cookies. Accordingly, the general data protection rules, as provided for by the Data Protection Law apply to online privacy as well.

Although there are no specific regulatory measures under the data protection regulatory framework, the Commissioner has tried to provide some clarifications on the notion of cookies and on their use, albeit in a minimalist way.

The Commissioner has defined the cookies in an online dictionary as *some data stored on the computer, which contain specific information.* This rudimentary definition is further complemented by a short explanation which states that cookies *allow any server to know what pages have been visited recently, just by reading them.*

In addition, the Commissioner has issued an opinion (which is slightly dated and as mentioned above does not have a binding effect on the data controllers) on the protection of personal data on the websites of public and private controllers. In this opinion the Commissioner reminds the data controllers on their obligations per the Data Protection Law and on the rights of data subjects, which apply to online personal data collection:

- The right to be fully informed and to give their approval if a website (or an application) processes their data;
- The right to keep their online communications secret (including email, the computer's IP or modem No.);
- The right to be notified if their personal data are compromised (data has been lost or stolen, or if their online privacy is likely to be negatively affected);
- The right to request that their personal data to be excluded from data processing for direct marketing if they have not given their consent.

Furthermore, in this opinion the Commissioner emphasizes the importance for data controllers to adopt privacy policies, which should include, *inter alia:*

- The identity of the controller;
- The information collected from the users, specifying the category of personal data;
- Specific policies regarding cookies and other technologies that allow data controllers to gather information on the users that use the website and to notify the latter about their use.

In addition to the above, it should be noted that the Electronic Communication Law (articles 124 -126), introduces rules on the processing of location data.

Under these rules, electronic communication providers may process traffic data only as long as such data is necessary for the purpose of the transmission of the communication’s transmission and thereafter must delete such data or render them anonymous.

Electronic communications service providers must provide in the contract entered into with the user details on the storage, the duration and the manner of processing of the traffic data. The Electronic Communication Law provides that these traffic data can be processed only by the relevant persons which are authorized by the electronic communications service providers, namely those who are responsible for billing or traffic management, customer service, marketing, fraud detection, or the provision of added value services, provided that the processing of traffic data should be limited only to the scope of their respective activity.

In addition, the Electronic Communication Law provides that the processing of location data can be carried out for the duration value added services and only if the data is rendered anonymous or if the user has granted their prior consent, which consent may be revoked at any time.

Prior to obtaining the consent of the users, the electronic communications service providers must provide information on:

- the type of location data to be processed;
- the purposes and duration of processing;
- the possibility that the location data be shared with third parties, for value-added service purposes.

The location data can be processed only by the relevant persons which are authorized by the electronic communications service providers, namely those who are responsible for the provision of the service or by third parties which are responsible for the provision of added value services, provided that the processing of traffic data should be limited only to the scope of their respective activity.

KEY CONTACTS

Tashko Pustina
tashkopustina.com/

Flonia Tashko
Partner
T +355423891 90
flonia.tashko@tashkopustina.com

Alban Shanaj
Partner
T +355423891 90
alban.shanaj@tashkopustina.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ALGERIA

Last modified 5 September 2024

LAW

Law No. 18-07 of 10 June 2018 on protection of natural persons in personal data processing (“**Law No. 18-07**”).

DEFINITIONS

Definition of Personal Data

Any information, regardless of the medium, relating to an identified or identifiable person, hereinafter referred to as "data subject", directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, genetic, biometric, mental, economic, cultural or social identity.

Definition of Sensitive Personal Data

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership of the data subject or relating to health, including genetic data.

NATIONAL DATA PROTECTION AUTHORITY

Since August 2023, an independent administrative authority for the protection of personal data, known as the "National Data Protection Authority" (**National Authority**), is hereby established, with its headquarters in Algiers.

The national authority is responsible for ensuring that the processing of personal data is carried out in accordance with the provisions of the law and for ensuring that the use of information and communication technologies does not threat the rights of individuals, public freedoms and privacy.

The National Authority’s missions are the below:

- Draw up rules of good conduct and ethics applicable to the processing of personal data;
- Advise individuals and entities in the use personal data;
- Inform data subjects of their rights and data controllers of their obligations;
- Issue authorizations and receive declarations relating to the processing of personal data;
- Authorize cross-border transfers of personal data under the conditions laid down by the law;
- Publish the authorisations granted and the opinions issued in the national register referred to in Article 28 of Law No. 18-07;
- Receive claims, appeals and complaints relating to the processing of personal data and inform their authors of the action taken on them;
- Order any changes necessary to protect the personal data processed;
- Order the closure, removal or destruction of data; and

- Take administrative sanctions under the conditions defined by Article 46 of the present law No. 18-07;

According to the statistics published by the National Authority, as of 31 October 2023, only 3 months after it began operations the achievements were the below:

- 228 files relating to declarations, requests for authorisation and requests for opinions submitted by bodies processing personal data had been received; and
- 174 files are awaiting further information, 54 files have been examined, including 46 declarations, 07 requests for authorisation and 01 request for an opinion, and the authority's overall mission is continuing.

More recently (i.e. on 28 February 2024), the National Authority announced on its website that it will begin its first field inspections of companies in the private sector, in order to examine the various processing procedures before extending the operation to individuals and public companies.

REGISTRATION

The National Authority has set up a digital portal on its website enabling those concerned by the processing of personal data to create an account and fill in electronic forms with the below:

- For prior declaration of processing operations;
- Requests for authorisation; and
- Requests for opinions.

Applicants may also monitor the status of their requests.

The processing of personal data is subject to the below:

- A prior declaration must be filed with the National Authority by the data controller of a private or public entity whenever the latter is likely to receive, store and process personal data. This declaration must be renewed before any new data is processed; or
- A prior authorization of the National Authority when the processing concerns any of the following:
    - transfer of personal data abroad;
    - communication of data to a third party;
    - The interconnection of data belonging to one or more legal entities managing a public service for different purposes relating to the general interest must be authorised by the National Authority;
        - Article 3 of the law No. 18-07 define “data interconnection” as (free translation): “ (…) *any mechanism of connection involving the linking of processed data for a specific purpose with other processed data, whether for identical or different purposes, by the same data controller or by one or more other data controllers.*”

DATA PROTECTION OFFICERS

Each natural or legal person processing personal data must designate its data controller or authorised representative and communicate the latter's contact details to the National Authority.

The form for appointing a representative is available on the portal of the National Authority's website.

The data controller shall implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

The data controller or its authorised representative will be considered the official contact for the National Authority.

In the case of a data officer established abroad:

In accordance with Article 04 (point 02) of Law No. 18-07 concerning the protection of individuals with regard to the processing of personal data (free translation):

> "When the data controller is not established in the Algerian territory but uses, for the purpose of processing personal data, automated or non-automated means located in the Algerian territory, excluding processing used solely for transit within the national territory.

> In this case, the data controller must notify the national authority of the identity of its representative established in Algeria, who, without prejudice to their personal responsibility, replaces them in all their rights and obligations arising from the provisions of this law and the texts adopted for its implementation."

As in any case, all the forms to be filled are available on the National Authority website or at direct request by e-mail to: contact.anpdp@anpdp.dz.

COLLECTION & PROCESSING

How is Personal Data collected

The law No. 18-07 applies to any public or private entity likely to receive, store and process personal data. As soon as an entity receives data, whether in digital form or not, it must comply with law No. 18-07.

Personal data is, notably, collected through direct input, cookies, social media, mobile apps, surveys, public records, purchase transactions, and by employers or institutions.

How is Personal Data processed

Personal data processing may only be processed with the express consent of the data subject (or consent of the legal representatives of a child, failing which by authorisation of the competent judge).

The data subject may withdraw his / her consent at any time.

Personal data may only be communicated to a third party for purposes directly related to the functions of the data controller and the recipient. Such communication is subject to the prior consent of the data subject.

However, in some cases, consent is not required if the processing is necessary:

- to comply with a legal obligation to which the data subject or the data controller is obliged;
- to protect the data subject's life;
- for the performance of a contract to which the data subject is a party or to the performance of pre-contractual measures taken at their request;
- to safeguard the vital interests of the person concerned, if they are physically or legally unable to give their consent;
- for the performance of a task carried out in the public interest. Or in the exercise of official authority vested in the data controller or the third party to whom the data is communicated; or
- for the accomplishment of a legitimate interest pursued by the data controller or the recipient, within the interest and/or fundamental rights and freedoms of the data subject.

Specific rights and protections

The person concerned by the collection of their data has a right to information, a right of access, a right of rectification and a right to object to their data being collected.

According to Article 9 of the law No. 18-07 (free translation):

“*Personal data must be:*

a. *processed lawfully and fairly;*
b. *collected for specified, explicit and legitimate purposes legitimate purposes and may not be further processed in a way that is incompatible with those purposes;*
c. *adequate, relevant and not excessive in relation to the purposes for which they are collected or processed;*
d. *accurate, complete and, where necessary, kept up to date;*
e. *kept in a form which permits identification of the data subjects for no longer than is the purposes for which they were collected or processed.*”

TRANSFER

According to the provisions of the law No. 18-07, the data controller may only transfer personal data to a foreign State with the authorisation of the national authority in accordance with Law No. 18-07 and if that State ensures an adequate level of protection of the privacy and fundamental rights and freedoms of individuals with regard to the processing of such data.

However, Article 45 of the law No 18-07 provides derogations from the general provisions for transferring personal data (free translation):

“*Article 45: In derogation from the provisions of Article 44 of this law [general provisions explained above], the data controller may transfer personal data to a State that does not meet the conditions specified in the said article [a sufficient level of protection for privacy and the fundamental freedoms and rights of individuals] under the following circumstances:*

1. *If the data subject has expressly consented to the transfer;*
2. *If the transfer is necessary for:*
    a. *Preserving the life of the data subject;*
    b. *Preserving public interest;*
    c. *Fulfilling obligations to establish, exercise, or defend a legal right;*
    d. *Executing a contract between the data controller and the data subject or for pre-contractual measures at the request of the data subject;*
    e. *Concluding or executing a contract in the interest of the data subject between the data controller and a third party;*
    f. *Executing a measure of international judicial cooperation;*
    g. *Preventing, diagnosing, or treating medical conditions.*
3. *If the transfer is carried out under a bilateral or multilateral agreement to which Algeria is a party.*
4. *With the authorization of the national authority, if the processing complies with the provisions of Article 2 of this law.*”

In any case, it is forbidden to communicate or transfer personal data to a foreign country, when such transfer is likely to affect public security or the vital interests of the State.

SECURITY

The controller must put in place measures to ensure the integrity and protection of the data.

These measures must ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

If the processing is carried out on behalf of the controller, the controller must choose a processor providing sufficient guarantees in respect of the technical and organisational security measures relating to the processing to be carried out and must ensure compliance with those measures.

Transfer of data abroad

The foreign State must ensure an adequate level of protection of the privacy and fundamental rights and freedoms of individuals with regard to data processing.

The adequacy of the level of protection provided by a State is assessed in particular by the security measures applicable there.

BREACH NOTIFICATION

Administrative measures

In case of violations of the provisions of Law No. 18-07 by the controller, administrative measures are taken by the national authority:

- warning;
- formal notice;
- provisional withdrawal for a period not exceeding one year, or definitive withdrawal of the declaration receipt or authorisation;
- a fine.

The national authority may also impose fines on the controller which:

- refuses, without legitimate reason, the rights of information, access, rectification or opposition;
- fails to make the required notifications to the national authority.

Criminal sanctions

Violation of the provisions of Law No. 18-07 is punishable by imprisonment and / or a fine.

Article 47 to 74 of the law No. 18-07 provide that non-compliance with the Data Protection Law is punishable by a fine ranging from 20,000 DZD to 1,000,000 DZD and / or imprisonment between two months and five years.

Mandatory breach notification

Where the processing of personal data over electronic communication networks results in the destruction, loss, alteration, disclosure or unauthorised access of such data, the service provider must notify the national authority and the data subject without delay where such a breach may affect the privacy of the data subject.

Failure by a service provider to notify the national authority or the data subject of a personal data breach is punishable by imprisonment and a fine.

ENFORCEMENT

Violation of the provisions of Law No. 18-07 is punishable by imprisonment and / or a fine.

Article 47 to 74 of the law No. 18-07 provide that non-compliance with the Data Protection Law is punishable by a fine ranging from 20,000 DZD to 1,000,000 DZD and / or imprisonment between two months and five years.

ELECTRONIC MARKETING

Law No. 18-05 of 10 May 2018 on electronic commerce provides that the e-provider who collects personal data and builds up customer and prospect files must only collect the data necessary to conclude commercial transactions. It must:

- collect the consent of e-consumers prior to the collection of data;
- guarantee the security of information systems and the confidentiality of data;
- comply with the relevant legislative and regulatory provisions.

ONLINE PRIVACY

Not applicable.

KEY CONTACTS

L& P Partners

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ANGOLA

Last modified 30 December 2021

LAW

Angola regulates data privacy and protection issues under the Data Protection Law (Law no. 22/11, 17 June 2011), the Electronic Communications and Information Society Services Law (Law no. 23/11, 20 June 2011) and the Protection of Information Systems and Networks Law (Law no. 7/17, 16 February 2017).

DEFINITIONS

Definition of personal data

The Data Protection Law defines personal data as any given information, regardless of its nature, including images and sounds related to a specific or identifiable individual.

An identifiable person is an individual directly or indirectly identified, notably, by reference to his or her identification number or to the combination of specific elements of his or her physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

The Data Protection Law defines sensitive personal data as personal data related to:

- Philosophical or political beliefs
- Political affiliations or trade union membership
- Religion
- Private life
- Racial or ethnic origin
- Health or sex life (including genetic data)

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Law establishes the *Agência de Proteção de Dados* (APD) as Angola’s data protection authority. APD’s Organic Statute was stablished by the Presidential Decree 214/2016 of October 10, and it’s board currently in office was nominated by the Presidential Decree 277/2019 September 6.

REGISTRATION

As provided by Law, entities shall provide prior notice to, or obtain prior authorization from, APD (depending on the type of personal data and purpose of processing) to process personal data. Please note that in the case of authorization, compliance with specific legal conditions is mandatory. APD has authority to exempt certain processing from notification requirements.

Generally, notification and authorization requests should include the following:

- The name and address of the controller and of its representative (if applicable)
- The purposes of the processing
- A description of the data subject categories and the personal data related to those categories
- The recipients or under which categories of recipient to whom the personal data may be communicated and respective conditions
- Details of any third party entities responsible for the processing
- The possible combinations of personal data
- The duration of personal data retention
- The process and conditions for data subjects to exercise their rights
- Any predicted transfers of personal data to third countries
- A general description (to allow APD to assess whether security measures adopted are suitable to protect personal data in its processing)

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

Generally, entities must obtain prior express consent from data subjects and provide prior notice to the APD to lawfully collect and process personal data. However, data subject consent is not required in certain circumstances provided by law.

To lawfully collect and process sensitive personal data, a legal provision must allow for processing and entities must obtain prior authorization from APD (please note that the authorization may only be granted in specific cases provided by law). If sensitive personal data processing results from a legal provision, APD must be provided with notice.

All data processing must follow these general principles: transparency, legality, good faith, proportionality, truthfulness and respect to private life as well as to legal and constitutional guarantees.

It is also mandatory that data processing is limited to the purpose for which the data is collected and that personal data is not held for longer than is necessary for that purpose.

There are specific rules applicable to the processing of personal data related to the following:

- Sensitive data on health and sexual life
- Illicit activities, crimes and administrative offenses
- Solvency and credit data
- Video surveillance and other electronic means of control
- Advertising by email
- Advertising by electronic means (direct marketing)
- Call recording

Specific rules for the processing of personal data within the public sector also apply.

TRANSFER

International transfers of personal data to countries with an adequate level of protection require prior notification to the APD. An adequate level of protection is understood as a level of protection equal to the Angolan Data Protection Law. APD decides which countries ensure an adequate level of protection by issuing an opinion to this respect.

International transfers of personal data to countries that do not ensure an adequate level of protection are subject to prior authorization from the APD, which will only be granted if specific requirements are met. For transfers between companies in the same group, the requirement of an adequate level of protection may be reached through the adoption of harmonized and mandatory internal rules on data protection and privacy.

Please note that the communication of personal data to a recipient, a third party or a subcontracted entity is subject to specific legal conditions and requirements.

SECURITY

Data controllers must implement appropriate technical and organizational measures and adopt adequate security levels to protect personal data from accidental or unlawful total or partial destruction, accidental loss, total or partial alteration, unauthorized disclosure or access (in particular where the processing involves the transmission of data over a network) and against all other unlawful forms of processing.

Such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, relative to the entities facilities and implementation costs. Specific security measures shall be adopted regarding certain type of personal data and purposes (notably, sensitive data, call recording and video surveillance).

Under the Protection of Information Systems and Networks Law, service providers, operators and companies offering information society services must: (i) guarantee the security of any device or set of devices used in the storage, processing, recovery or transmission of computer data on execution of a computer program and (ii) promote the registration of users as well as the implementation of technical measures in order to anticipate, detect and respond to risk situations. The Law requires an accident and incident management plan in case of a computer emergency.

BREACH NOTIFICATION

There is no mandatory breach notification requirement under the Data Protection Law.

However, pursuant to the Electronic Communications and Information Society Services Law, companies offering electronic communications services accessible to the public shall, without undue delay, notify the APD and the Electronic Communications Authority, *Instituto Angolano das Comunicaçõ*es, (INACOM) of any breach of security committed with intent or that recklessly leads to destruction, loss, partial or total modification or non-authorized access to personal data transmitted, stored, retained or in any way processed under the offer of electronic communications services.

Companies offering electronic communications services accessible to the public shall also keep an accurate register of data breaches, indicating the concrete facts and consequences of each breach and the measures put in place to repair or prevent the breach.

The same applies under Protection of Information Systems and Networks Law.

ENFORCEMENT

Data protection

As mentioned above, the competent authority for the enforcement of Data Protection Law is the APD. However, considering that the APD was recently created, the level of enforcement is not significant at this stage.

Electronic communications

INACOM regulates and monitors compliance with the Electronic Communications and Information Society Services Law, and issues penalties for its violation. Presently, INACOM’s level of enforcement is not yet significant.

ELECTRONIC MARKETING

The dissemination of electronic communications for advertising purposes is generally subject to the prior express consent of its recipient (opt-in) and to prior notification to APD.

Entities may process personal data for electronic marketing purposes without data subject consent in specific circumstances, notably:

- When advertising is addressed to the data subject as representative employee of a corporate person, and
- When advertising communications are sent to an individual with whom the product or service supplier has already concluded a transaction, provided an opportunity to refuse consent was expressly provided to the customer at the time of the transaction at no additional cost.

ONLINE PRIVACY

The Electronic Communications and Information Society Services Law establishes the right of all Citizens to enjoy protection against abuse or violations of their rights through the Internet or other electronics means, such as:

- The right to confidentiality of communications and to privacy and non-disclosure of their data
- The right to security of their information by improvement of quality, reliability and integrity of the information systems
- The right to security on the Internet, specifically for minors
- The right not to receive spam
- The right to the protection and safeguarding of their consumer rights and as users of networks or electronic communications services

In view of the above, entities are generally prohibited from storing any kind of personal data without prior consent of the user. This does not prevent technical storage or access for the sole purpose of carrying out the transmission of a communication over an e-communication network or if strictly necessary in order for the provider of an information society service to provide a service expressly requested by the subscriber or user.

Traffic data

The processing of traffic data is allowed when required for billing and payment purposes, but processing is only permitted until the end of the period during which the bill may lawfully be challenged or payment pursued. Traffic data must be eliminated or made anonymous when no longer needed for the transmission of the communication.

The storage of specific information and access to that information is only allowed on the condition that the subscriber or user has provided his or her prior consent. The consent must be based on accurate, clear and comprehensive information, namely about the type of data processed, the purposes and duration of the processing and the availability of data to third parties in order to provide value added services.

Electronic communications operators may store traffic data only to the extent required and for the time necessary to market electronic communications services or provide value added services. Prior express consent is required and such consent may be withdrawn at any time.

Processing should be limited to those employees in charge of:

- Billing or traffic management
- Customer inquiries
- Fraud detection
- Marketing of electronic communications
- Services accessible to the public
- The provision of value added services

Notwithstanding the above, electronic communication operators should keep in an autonomous file all traffic and localization data exclusively for the purpose of:

- Investigation
- Detection, or
- Prosecution of criminal offenses on Information and Communication Technologies (ICT)

Location data

Location Data processing is only allowed if the data is made anonymous or to the extent and for the duration necessary for the provision of value added services, provided prior express consent is obtained. In this case, prior complete and accurate information must be provided on the type of data being processed, as well as the purposes and duration of processing and any possibility of disclosure to third parties for the provision of value added services.

Electronic communication operators must ensure that data subjects have the opportunity to withdraw consent, or temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication, at any time. The withdrawal mechanism must be provided through simple means, free of charge to the user. Processing should be limited to those employees in charge of electronic communications services accessible to the public.

KEY CONTACTS

ACDA

Joni Garcia
Associate
ACDA
T +244 926 61 25 25
j.garcia@adca-angola.com

Murillo Costa Sanches
Of Counsel
ACDA
T +244 926 61 25 25
m.sanches@adca-angola.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ARGENTINA

Last modified 28 January 2024

LAW

Article 43 of the Federal Constitution, third paragraph, provides, in relevant part that any person may file an action to have access to personal data about such person and to information about the purpose with which they are kept, included in public data registries or banks, or in private data registries or banks, and to request the suppression, correction, confidentiality or updating of the data where inaccurate or discriminatory.

These provisions do not create an express constitutional right to privacy or data protection, but do create the basic framework for the protection of such right, as well as the foundation for the legislation, subsequently enacted, which regulates the details of that protection.

Law 25,326 - the Personal Data Protection Law (PDPL) includes the basic personal data rules. It follows international standards, and has been considered as granting adequate protection by the European Commission. Decree 1558 of 2001 includes regulations issued under the PDPL. Further regulations have been issued by the relevant agencies.

In November 2022, Argentina ratified Decision 108 of the Council of Europe, as amended, by means of Law 27,699.

DEFINITIONS

Definition of personal data

Personal data is defined as information of any type referred to individuals or legal entities, determined or which may be determined.

Definition of sensitive personal data

Sensitive data includes personal data which reveal racial or ethnic origin, political opinions, religious, philosophical or moral convictions, trade union affiliation and information related to health and sexual activities.

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to Decree 746 of 2017, it is the Agency for Access to Public Information (Agencia de Acceso a la Información Pública).

REGISTRATION

All archives, registries, databases and data banks, whether public or private, having the purpose of supplying information, must be registered with the Registry organized by the national data protection authority. This registration requires the following information, to be provided to the registry:

- The name and domicile of the person responsible for the archive, registry, database or data bank
- The characteristics and purpose of the archive, registry, database or data bank
- The nature of the personal data included or to be included in the archive, registry, database or data bank
- The way in which data are collected and updated
- The destination of the data and the identity of the individuals or legal entities to whom such data may be transferred
- The way in which the recorded information is interrelated
- The means to assure the security of the data, indicating the category of persons with access to the processing of data
- The term during which the data will be preserved
- The way and conditions pursuant to which interested persons may have access to the data referring to such persons, and the procedures to be followed to rectify and update the registered data

DATA PROTECTION OFFICERS

Generally, there is no specific requirement to appoint a data protection officer. Under certain circumstances, in which special security standards apply, it may be necessary to appoint an officer in charge of data security.

COLLECTION & PROCESSING

Personal data collected for purposes of processing must be truthful, adequate, relevant and not excessive in relation with the scope and purpose for which they were obtained. The gathering of data shall not take place by unfair or fraudulent means or in an otherwise illegal manner.

Personal data may not be used for purposes different from or incompatible with those for which the personal data was initially collected. Personal data must be accurate and properly updated when necessary. Totally or partially inaccurate personal data, or those that are incomplete, shall be suppressed and substituted, or completed where relevant, by the person responsible for the archive or database, whenever such person becomes aware of the inaccurate or incomplete character of the information.

Consent from the data subject is required, which must be free, express and informed consent and in writing or in another equivalent form, unless:

- The personal data were obtained from sources open to unrestricted public access
- The personal data were obtained as part of the performance of state duties or in compliance with a legal obligation
- The personal data consists of lists whose data are limited to the name, national identity document number, tax or social security identification, occupation, date of birth and domicile
- The personal data are derived from a contractual, scientific or professional relationship and are necessary for such relationship
- The personal data result from operations conducted by financial entities with their clients or consist in the information such financial entities receive from their clients pursuant to the Financial Entities Law

When the authorization for the collection and processing of data is requested, the data subject must be informed about the purpose for which the data will be processed, as well as about the individuals or groups of individuals who will have access to the processed information. In addition, the archive, registry or data bank where the information will be kept must be identified, together with the person responsible for it. The data subject must be informed about the voluntary or compulsory nature of the

answers requested from such owner, as well as about the consequences of providing the personal data or of refusing to give such information or of providing untruthful information. The data subject must also be informed about the right to access, rectify and suppress the relevant data.

Special rules apply to sensitive data. No person may be required to disclose sensitive data. Sensitive data may only be collected and processed where necessary, and with consent, as expressly permitted by law, or for statistical or scientific purposes provided the person they refer to may not be identified.

Data related to criminal records may only be processed by the relevant public authorities.

TRANSFER

Transfers and disclosures to third parties

Personal data may only be transferred for legitimate purposes of the transferor and the transferee, and generally with the prior consent of the data subject who must be informed of the transfer’s purpose and of the transferee’s identity. This consent may be rescinded.

Consent is not required in the case of transfer of data regarding which consent was not necessary for collection. Also, it is not necessary in the case of transfer of data between state agencies, for purposes of performance of their respective activities, on in connection with health-related data, if the transfer is necessary for public health or emergency reasons, or for the performance of epidemiological studies, provided the identity of the persons to whom such data refer is reserved by means of adequate dissociation mechanism. In addition, consent is not necessary, for personal data generally, if an adequate dissociation mechanism is used in a way such that the data subjects are not identifiable.

Cross-border transfers

The cross-border transfer of personal data is prohibited to countries or international or supranational organization which do not provide adequate protection to such data, unless:

- The data subjects expressly consents to that transfer
- The transfer is necessary for international judicial cooperation
- The transfer takes place as part of certain exchanges of medical data
- Bank or stock exchange transfers, in the context banking or stock exchange transactions
- The transfer takes place as provided in the context of international treaties to which Argentina is a party
- The transfer has as its purpose the international cooperation between intelligence agencies engaged in combating organized crime, terrorism and drug traffic

SECURITY

The person responsible for a data archive, or using such archive, must adopt the technical and organizational measures to assure the security and confidentiality of personal data, so as to avoid their adulteration, loss, consultation or non-authorized processing, and to detect the misuse of information. The recording of personal data in archives, registries or data banks that do not comply with the legal requirements on integrity and security is prohibited.

BREACH NOTIFICATION

Not specifically required under data protection law.

Failure to notify a data security breach is not in itself a violation of the data protection regime, but may bear on the effects of security violation, especially if lack of such notification results in other security breaches or damages. The person responsible for the data must keep records on security breaches, and these records may be requested by the data protection authority.

Breach notification may be mandatory if the data protection authority specifically requests information about data breaches.

ENFORCEMENT

There are several enforcement mechanisms:

- The data protection authority may enforce the legal provisions and regulations on data protection, imposing fines in case of violation.
- Violation of data protection rules may constitute a crime subject to prison terms imposed by criminal courts.
- Court actions may be brought to have access to personal data and to request their correction, suppression, confidentiality or updating.

ELECTRONIC MARKETING

Electronic marketing, to the extent that it may involve processing of personal data, is subject to the general rules applicable to such data, such as valid data subject consent, adequate privacy notices as to use and disclosure of personal data and data subject rights.

ONLINE PRIVACY

Although there are no detailed regulations on online privacy, the general rules on privacy provided by the Civil and Commercial Code are applicable in this context. Nuisances from unrequested communications may be actionable. Unauthorized collection of personal data will be subject to the general rules applicable to such data.

KEY CONTACTS

Guillermo Cabanellas
Senior Partner
T +5411 41145500
g.cabanellas@dlapiper.ar

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ARMENIA

Last modified 17 January 2024

LAW

Personal Data Protection Law as of 18.05.2015, number ՀՕ-49-Ն.

DEFINITIONS

Personal Data is defined as *any information related to an individual that allows or may allow directly or indirectly identifying a person.*

Definition of Sensitive Personal Data

Special Category is defined as any information related to a person's։

- race;
- nationality or ethnicity;
- political views;
- religious or philosophical beliefs;
- membership in a professional union;
- health status; and
- sexual life.

Definition of Personal Life Data

Data on personal life is defined as any information on a person’s:

- personal life;
- family life;
- the physical, physiological, mental, or social condition of a person; or
- other similar information.

Definition of Biometric Personal Data

Biometric personal data is defined as any information characterizing person’s

- the physical characteristics;
- physiological characteristics; and / or
- biological characteristics of a person.

Definition of Publicly Available Personal Data

Publicly available personal data shall mean information, which, by the data subject's consent or by conscious operations aimed at making his or her personal data publicly available, becomes publicly available for a certain scope of persons or the public at large, as well as information, which is provided for by law as publicly available information.

NATIONAL DATA PROTECTION AUTHORITY

Based on Decision N 573-A of the RA Prime Minister as of July 3, 2015, the Personal Data Protection Agency of the RA Ministry of Justice was appointed as the authorized body for personal data protection.

REGISTRATION

Registration is voluntary unless otherwise specified by the authorized body. Processing of personal data may be carried out by state administration or local self-government bodies, state or municipal institutions or organizations, legal or natural persons, which organize and / or carry out the processing of personal data.

The processor, prior to the processing of personal data, shall have the right to notify the authorized body for the protection of personal data of the intention to process data.

At the request of the authorized body, the processor shall be obliged to send a notification to the authorized body.

The processor, prior to the processing of biometric or special category personal data, shall be obliged to notify the authorized body for the protection of personal data of the intention to process data.

The notification shall include the following information:

- name (surname, name, patronymic) of the processor or his or her authorised person (if any), registered office or place of registration (actual residence);
- purpose and legal grounds for processing personal data;
- scope of personal data;
- scope of data subjects;
- list of operations performed upon personal data, general description of the ways of processing personal data by the processor;
- description of measures which the processor is obliged to undertake for ensuring security of processing personal data;
- date of starting the processing of personal data;
- time limits and conditions for completing the processing of personal data.

The authorized body for the protection of personal data shall enter the information mentioned in the notification, as well as the information on the date of sending the given notification into the register of processors within thirty days following the receipt of the given notification.

In case when information submitted by the processor, provided for by the mentioned notification, is incomplete or inaccurate, the authorized body for the protection of personal data shall have the right to require the processor to specify the submitted information prior to its entry into the register of processors.

DATA PROTECTION OFFICERS

No requirement to appoint a data protection officer.

COLLECTION & PROCESSING

- By and large, the entities must obtain prior express consent from data subjects to lawfully collect and process personal data․ The consent is not necessary in the cases directly provided by the legislation or if the data is being collected from public sources.

- The data subject may give his or her consent in person or through the representative, where the power of attorney specifically provides for such a power.
- The data subject's consent shall be considered to be given and the processor shall have the right to process, where:
  - personal data are indicated in a document addressed to the processor and signed by the data subject, except for the cases when the document, by its content, is an objection against processing of personal data;
  - the processor has obtained data on the basis of an agreement concluded with the data subject and uses it for the purposes of operations prescribed by this Agreement;
  - the data subject, voluntarily, for use purposes, verbally transfers information on his or her personal data to the processor.
- Personal data may be processed without the data subject's consent, where the processing of data is directly provided for by law.
- The processor of personal data or the authorised person, for obtaining the data subject's written consent, shall notify the data subject of the intention to process the data.
- The data subject shall give his or her consent in writing or electronically, validated by electronic digital signature; in case of an oral consent — by means of such reliable operations which will obviously attest the consent of the data subject on using the personal data.

The processor of personal data for obtaining the data subject's consent notifies of the intention to process the data. The notification shall include:

- surname, name, patronymic of the data subject;
- legal grounds and purpose of the processing of personal data;
- list of personal data subject to processing;
- list of operations to be performed upon personal data for which the subject's consent is requested;
- scope of persons to whom personal data may be transferred;
- name (surname, name, patronymic, position) of the processor or his or her representative requesting the data subject's consent and registered office or place of registration (actual residence);
- information on requiring by the data subject rectification, destruction of personal data, terminating the processing of data or on carrying out other operation relating to the processing;
- validity of the consent requested, as well as the procedure and consequences of withdrawing the consent.

Characteristics for processing publicly available personal data

- A regime of publicly available information of personal data (phone directories, address books, biographical directories, private announcements, declaration of income, etc.) may be established by the data subject's consent or in cases provided for by law. The name, surname, year, month and day of birth, place of birth, place of death, year, month and day of death, as well as the personal data which by conscious operations carried out by the data subject aimed at making publicly available becomes publicly available for certain scope of persons or public at large, shall be considered as publicly available.
- Information on the data subject, except for information provided for by previous clause, may be removed from publicly available sources of personal data at the request of data subject or through judicial procedure.
- The data being processed on the basis of an agreement may be removed from publicly available sources of personal data by mutual consent or through judicial procedure.

Characteristics for processing sensitive personal data

- The processing of special category personal data without the person's consent shall be prohibited, except when the processing of data is directly provided for by law.
- The processing of personal data provided for by the previous clause shall immediately be terminated, where the grounds and purpose of the processing of data were eliminated.

Characteristics for processing personal data of persons with incapacity or limited capacity and minors under the age of 16

In case of incapacity or limited capacity of the data subject or of being a minor under the age of 16, consent for processing his or her personal data shall be given by a legal representative / parent of the data subject

Characteristics for processing biometric personal data

Biometric personal data shall be processed only by the data subject's consent, except for cases provided for by law and where the purpose pursued by law is possible to implement only through processing of these biometric data.

Processing of personal data by an authorized person assigned by the processor of data

Personal data may also be processed by an authorized person assigned by the processor. The assignment shall be in writing, which shall include

- legal grounds and conditions;
- the purpose of the processing of personal data;
- the list of personal data subject to processing;
- the scope of data subjects;
- the scope of persons to whom personal data may be transferred;
- technical and organizational measures for the protection of personal data and other necessary information.

Personal data shall be processed only within the scope of the assignment. The processor of data shall be responsible for the processing of personal data within the scope of the assignment. Where the assignment does not comply with the requirements of the Law, the authorized person must inform in writing thereon to the processor of data and refuse the processing.

Blocking or destruction of personal data

The data subject shall have the right to get familiarized with his or her personal data, and require the processor to rectify, block or destruct his or her personal data, where the personal data are not complete or accurate or are outdated or has been obtained unlawfully or are not necessary for achieving the purposes of the processing.

In case of doubts with regard to the rectification, blocking or destruction of personal data by the processor, the data subject shall have the right to apply to the authorized body for the protection of personal data to make clear the fact of his or her personal data being rectified, blocked or destructed and by the request to be provided with information.

In case of incomplete, inaccurate, outdated, unlawfully obtained personal data or those unnecessary for achieving the purposes of the processing, the processor of personal data shall be obliged to carry out necessary operations for making them complete, keeping up to date, rectifying or destructing.

The processor shall be obliged to destruct or block personal data that are not necessary for achieving the legitimate purpose.

TRANSFER

Transfer to third parties shall mean an operation aimed at transferring personal data to a certain scope of persons or the public at large or at familiarizing with them, including disclosure of personal data through the mass media, posting in information communication networks or otherwise making personal data available to another person.

The processor may transfer personal data to third parties or grant access to data without the personal data subject's consent, where it is provided for by law and has an adequate level of protection.

The processor may transfer special category personal data to third parties or grant access to data without the personal data subject’s consent, where:

- the data processor is considered as a processor of special category personal data prescribed by law or an interstate agreement, the transfer of such information is directly provided for by law and has an adequate level of protection;

- in exceptional cases provided for by law special category personal data may be transferred for protecting life, health or freedom of the data subject.

Personal data may be transferred to another country with the data subject's consent or where the transfer of data stems from the purposes of processing personal data and/or is necessary for the implementation of these purposes.

Personal data may be transferred to another state without the permission of the authorized body, where the given state ensures an adequate level of protection of personal data. An adequate level of protection of personal data shall be considered to be ensured, where:

- personal data are transferred in compliance with international agreements;
- personal data are transferred to any of the countries included in the list officially published by the authorized body.

Personal data may be transferred to the territory of the State not ensuring an adequate level of protection only by the permission of the authorized body where personal data are transferred on the basis of an agreement, and the agreement provides for such safeguards with regard to the protection of personal data which were approved by the authorized body as ensuring adequate protection.

In cases referred to in the previous paragraph the processor of personal data shall be obliged — prior to the transfer of data to another country — to apply to the authorized body to obtain permission. The processor of personal data shall be obliged to specify in the application the country where personal data are transferred, the description of the recipient of personal data (name, legal form), the description (content) of personal data, the purpose of processing and transferring personal data, agreement or the draft thereof. The authorized body shall be obliged to permit or reject the application within 30 days. The authorized body may require from the processor of personal data additional information by observing the time limit for the consideration of the application. In case when the authorized body finds that contractual safeguards are not sufficient, it shall be obliged to specify those necessary changes which will ensure safeguards for the protection of personal data.

Personal data under the disposition of state bodies may be transferred to foreign state bodies only within the scope of interstate agreements, whereas to non-state bodies in accordance with the norms provided above.

SECURITY

The processor has an obligation to destruct or block personal data that are not necessary for achieving the legitimate purpose.

In the course of processing personal data, the processor shall be obliged to use encryption keys to ensure the protection of information systems containing personal data against accidental loss, unauthorized access to information system, unlawful use, recording, destructing, altering, blocking, copying, and disseminating personal data and other interference.

The processor is obliged to prevent the access of appropriate technologies for processing personal data for persons not having a right thereto and ensure that only data, subject to processing by him or her, are accessed by the lawful user of these systems and the data which are allowed to be used.

The requirements for ensuring security of processing of personal data in information systems, the requirements for tangible media of biometric personal data and technologies for storage of these personal data out of information systems shall be prescribed by the decision of the government of the Republic of Armenia. In case another body exercising control is prescribed by law, this body, within the scope of powers reserved to it by law, may prescribe higher requirements other than those provided above.

Use and storage of biometric personal data out of information systems may be carried out only through such tangible media, application of such technologies or forms, which ensure the protection of these data from the unauthorized access thereof, unlawful use, destruction, alteration, blocking, copying, dissemination of the personal data, etc.

Processors of personal data or other persons provided for by this law shall be obliged to maintain confidentiality both in the course of performing official or employment duties concerning the processing of personal data and after completing thereof.

The control over the fulfillment of the above-mentioned requirements shall be exercised by the authorized body for the protection of personal data without the right to process personal data being processed in the information systems.

Legal persons processing personal data, for having recognized electronic systems for processing the personal data under their possession as having an adequate level of protection and including them in the register, may apply to the authorized body for the protection of personal data.

BREACH NOTIFICATION

In case unlawful operations performed upon personal data are revealed, the processor shall be obliged to immediately, but not later than within three working days eliminate the committed violations. In case it is impossible to eliminate the violations, the processor shall be obliged to immediately destruct personal data. The processor shall be obliged to inform the data subject or his or her representative on the elimination of violations or the destruction of personal data within three working days, and where the request is received from the authorized body for the protection of personal data — also this body.

The processor shall be obliged to inform the data subject or his or her representative on the elimination of violations or the destruction of personal data within three working days, and where the request is received from the authorized body for the protection of personal data — also this body.

Mandatory breach notification

In case of an outflow of personal data from electronic systems the processor shall be obliged to immediately publish an announcement thereon, meanwhile reporting on the outflow the Police of the Republic of Armenia and authorized body for the protection of personal data.

ENFORCEMENT

The authorized body for the protection of personal data is entitled to:

- check, on its initiative or on the basis of an appropriate application, the compliance of the processing of personal data with the requirements of this Law;
- apply administrative sanctions prescribed by law in the case of violation of the requirements of this Law;
- require blocking, suspending or terminating the processing of personal data violating the requirements of this Law;
- require from the processor rectification, modification, blocking or destruction of personal data where grounds provided for by this Law exist;
- prohibit completely or partially the processing of personal data as a result of examination of the notification of the processor on processing personal data;
- keep a register of processors of personal data;
- recognize electronic systems for processing of personal data of legal persons as having an adequate level of protection and include them in the register;
- check the devices and documents, including the existing data and computer software used for processing data;
- apply to court in cases provided for by law;
- exercise other powers prescribed by law;
- maintain the confidentiality of personal data entrusted or known to it in the course of its activities;
- ensure the protection of rights of the data subject;
- consider applications of natural persons regarding the processing of personal data and deliver decisions within the scope of its powers;
- submit, once a year, a public report on the current situation in the field of personal data protection and on the activities of the previous year;
- conduct researches and provide advice on processing data on the basis of applications or coverages of processors or inform on best practices on processing of personal data;
- report to law enforcement bodies where doubts arise with regard to violations of criminal law nature in the course of its activities.

ELECTRONIC MARKETING

There is no regulation. However, it is advised to obtain user consent, such as through appropriate disclaimers.

ONLINE PRIVACY

There is no regulation on cookies and location data. However, it is advisable to obtain user consent, such as through appropriate disclaimers.

KEY CONTACTS

LEGELATA Law Firm
legelata.am/

Arthur Buduryan
Partner
LEGELATA Law Firm
T +37495993696
arthur.buduryan@legelata.am

Artyom Poghosyan
Associate
LEGELATA Law Firm
T +37495992636
artyom.poghosyan@legelata.am

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ARUBA

Last modified 28 January 2024

LAW

- **National Ordinance Person Registration** (*Landsverordening persoonsregistratie*, National Gazette 2011, Consolidated text no. 37) (“National Ordinance Person Registration”);
- **General Data Protection Regulation** (the “GDPR”) – a regulation of the European Union which became effective on May 25, 2018 – may have implications for a data controller / data processor as the extra-territorial reach of the GDPR is not only relevant to businesses established in the European Union but also to international businesses established in Aruba which offer goods or services to individuals in the European Union or monitor their behaviour in the European Union.

DEFINITIONS

Definition of Personal Data

National Ordinance Person Registration

According to the Explanatory Memorandum on the National Ordinance Person Registration the term personal data has a broad meaning. This does not only concern data that can identify a person, but concerns any data that can be associated with a particular person; it is foreseeable that under certain circumstances data can be traced to one person through systematic comparison and lengthy investigations. Personal identifiable confidential data is therefore not only limited to home address, email address, telephone number, membership number and/or identity number.

GDPR

Personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Definition of Sensitive Personal Data

National Ordinance Person Registration

Religion or belief, race, political opinion, sexuality, as well as personal data of a medical, psychological or disciplinary nature, and personal data concerning the trade union membership.

GDPR

Data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

NATIONAL DATA PROTECTION AUTHORITY

National Ordinance Person Registration

Public prosecutor.

GDPR

An independent public authority established by a Member state pursuant to article 51 of the GDPR (Article 4(21), GDPR). The authority is responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the EU.

REGISTRATION

National Ordinance Person Registration

No registration required.

GDPR

Article 30 GDPR requires companies to keep an internal electronic registry, which contains the information of all personal data processing activities carried out by the company.

DATA PROTECTION OFFICERS

National Ordinance Person Registration

Pursuant to article 8 of the National Ordinance Person the data controller shall execute appropriate technical and organizational measures to secure personal data against loss or violation of the data against unauthorized access, change or transmission thereof.

Besides the measures above, the National Ordinance Person Registration does not contain any clauses on appointing a mandatory data protection officer.

GDPR

The appointment of a data protection officer under the GDPR is only mandatory in three situations:

- When the organisation is a public authority or body;
- If the core activities require regular and systematic monitoring of data subjects on a large scale; or
- If the core activities involve large scale processing of special categories of personal data and data relating to criminal convictions.

COLLECTION & PROCESSING

National Ordinance Person Registration

Collection: a natural or legal person, public authority, agency or other body which who has control over a person registration.

Processor: a natural or legal person, public authority, agency or other body which who owns all or part of the has equipment in his possession, with which a personal registration of which he is not the holder.

GDPR

Collection: a natural or legal person, public authority, agency or other body that collect personal data and use it for certain purposes, like a website that markets to users based on their online behaviour.

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority.

TRANSFER

National Ordinance Person Registration

By means of article 9 of the National Ordinance Person Registration, recorded data will only be made available to third parties in accordance with the purpose of the register and if obligated by law or done with the consent of the registered persons.

GDPR

The GDPR restricts transfers of personal data outside the European Economic Area, or the protection of the GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.

SECURITY

National Ordinance Person Registration

Pursuant to article 8 of the of the National Ordinance person Registration the data controller shall execute appropriate technical and organizational measures to secure personal data against loss or violation of the data against unauthorized access, change or transmission thereof.

GDPR

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (article 32 GDPR).

BREACH NOTIFICATION

National Ordinance Person Registration

Contains no specific clauses.

GDPR

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with article 55 GDPR, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

ENFORCEMENT

National Ordinance Person Registration

Pursuant to article 20 of the National Ordinance person registration, the individual violating the provisions of the national ordinance person registration can be punished with a maximum fine of Afl.10.000. (USD. 5586.59).

GDPR

The GDPR holds a variety of potential penalties for businesses.

For example, article 77 of GDPR states that:

“Every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating him or her infringes this Regulation.”

Additionally, article 79 of the Regulation states that *“such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence.”*

Penalties

Compensation to Data Subjects. One penalty that may be imposed is compensation to, as stated in article 82 of the Regulation, *“Any person who has suffered material or non-material damage as a result of an infringement of this Regulation”* for the damage they’ve suffered.

Fines

Article 83 of GDPR specifies a number of different fines that may vary based on the nature of the infraction, its severity, and the level of cooperation that “data processors” (i.e. you) provide to the “supervisory authority.” Less severe infringements may incur administrative fines of up to 10,000,000 Euros or 2% of your total worldwide annual turnover for the preceding year (whichever is greater), while more severe infractions may double these fines (20,000,000 or 4% annual turnover).

Individual Member States of the EU may have additional fines and penalties that may be applied as well. However, these additional penalties are not specifically listed in the text of the Regulation since they’re up to the individual EU nations to set— the only guidelines in article 84 of GDPR are that “*Such penalties shall be effective, proportionate and dissuasive”* and that “*Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018.”*

ELECTRONIC MARKETING

National Ordinance Person Registration

N/A

GDPR

Under article 22 GDPR organizations cannot send marketing emails without active, specific consent.

Companies can only send email marketing to individuals if:

- The individual has specifically consented.
- They are an existing customer who previously bought a similar service or product and were given a simple way to opt out.

ONLINE PRIVACY

National Ordinance Person Registration

Contains no specific clauses.

GDPR

Cookies, insofar as they are used to identify users, qualify as personal data and are therefore subject to the GDPR. Companies do have a right to process their users’ data as long as they receive consent or if they have a legitimate interest.

Location data, the GDPR will apply if the data collector collects the location data from the device and if it can be used to identify a person.

If the data is anonymized such that it cannot be linked to a person, then the GDPR will not apply. However, if the location data is processed with other data related to a user, the device or the user’s behavior, or is used in a manner to single out individuals from others, then it will be “personal data” and fall within the scope of the GDPR even if traditional identifiers such as name, address etc. are not known.

KEY CONTACTS

HBN Law & Tax
hbnlawtax.com/

Maarten Willems
Senior Associate
HBN Law & Tax
T +297 588 6060
maarten.willems@hbnlawtax.com

Misha Bemer
Partner
HBN Law & Tax
T +297 588 6060
misha.bemer@hbnlawtax.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

AUSTRALIA

Last modified 31 December 2023

LAW

Australia regulates data privacy and protection through a mix of federal, state and territory laws. The federal Privacy Act 1988 (*Cth*) ("**Privacy Act**") and the Australian Privacy Principles ("**APPs**") contained in the Privacy Act apply to private sector entities (including body corporates, partnerships, trusts and unincorporated associations) with an annual turnover of at least AU$3 million, and all Commonwealth Government and Australian Capital Territory Government agencies.

The Privacy Act regulates the handling of personal information by relevant entities and under the Privacy Act, the Information Commissioner has authority to conduct investigations, including own motion investigations, to enforce the Privacy Act and seek civil penalties for serious and egregious breaches or for repeated breaches of the APPs where an entity has failed to implement remedial efforts.

The Privacy Act is currently undergoing a review and the Attorney General’s Department released the Privacy Act Review Report 2022 setting out 116 proposed amendments to the Privacy Act. The Government Response to the Privacy Act Review Report released in 2023 indicated that of the 116 recommendations, the Australian Government “agreed” to 38 of them, “agreed in principle” to another 68 and rejected 10. The timing for the implementation of these changes is not yet clear, however, it is likely that this will be undertaken during 2024 – 2025 and that any revisions will result in more prescriptive and onerous requirements being imposed on organisations handling personal information of Australian residents.

In late 2023, appointments were made of a separate Privacy Commissioner and Freedom of Information Commissioner - these roles were all performed by the Information Commissioner. The Privacy Commissioner will perform the privacy functions which relate to the privacy of individuals with both new appointments beginning in February 2024.

Most States and Territories in Australia (except Western Australia and South Australia) have their own data protection legislation applicable to relevant State or Territory government agencies, and private businesses that interact with State and Territory government agencies. These Acts include:

- *Information Privacy Act 2014* (Australian Capital Territory)
- *Information Act 2002* (Northern Territory)
- *Privacy and Personal Information Protection Act 1998* (New South Wales)
- *Information Privacy Act 2009* (Queensland)
- *Personal Information Protection Act 2004* (Tasmania), and
- *Privacy and Data Protection Act 2014* (Victoria)

Additionally, there are other parts of State, Territory and federal legislation that relate to data protection. For example, the following all impact privacy and data protection for specific types of data or activities: the *Telecommunications Act 1997* (*Cth*), the *Criminal Code Act 1995* (*Cth*), the *National Health Act 1953* (*Cth*), the *Health Records and Information Privacy Act 2002* (NSW), the *Health Records Act 2001* (Vic) and the *Workplace Surveillance Act 2005* (NSW).

Specific regulators have also expressed an expectation that regulated entities should have specified data protection practices in place. For example, the Australian Prudential and Regulatory Authority ("**APRA**"), which regulates financial services institutions requires regulated entities to comply with Prudential Standards, including Prudential Standard CPS 234 Information Security (" **CPS 234**"), and the Australian Securities and Investment Commission regulates corporations more generally.

Other important privacy and data protection laws

Assistance and Access Act

The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)* ("**AA Act**") provides law enforcement agencies with access to encrypted data for serious crime investigation and imposes obligations on "Designated Communications Providers". However, the AA Act may inadvertently have a much broader remit with limited judicial oversight, and has been the subject of much criticism from local and global technology firms which have stated the legislation has the potential to significantly impact security / encryption solutions in Australia.

The AA Act allows various agencies to do any of the following:

- Issue a "technical assistance notice", which requires a communications provider to give assistance that is reasonable, proportionate, practicable and technically feasible;
- Issue a "technical capability notice", which requires a communications provider to build new capabilities to assist the agency. The Attorney-General must consult with the communications provider prior to issuing the notice, and must be satisfied that the notice is reasonable, proportionate, practicable and technically feasible; and
- Make "technical assistance requests", to give foreign and domestic communications providers and device manufacturers a legal basis to provide voluntary assistance to various Australian intelligence organizations and interception agencies relating to issues of national interest, national security and law enforcement.

Organizations will need to ensure customer terms and conditions deal carefully with the matter of legal compliance and any commitments made to customers generally.

Security of Critical Infrastructure Act

The *Security of Critical Infrastructure Act 2018 (Cth)* ("**SOCI Act**") applies to organisations that own or operate (or hold a direct interest in) assets in a range of sectors including communications, energy, defence, financial services, transport, data processing or storage, supermarket / grocery supply chains, health and medical, education and space.

The key obligations under the SOCI Act include:

- Organisations must provide “operational” and ownership information to the Cyber Infrastructure Security Centre for inclusion on the Register of Critical Infrastructure Assets, in accordance with the requirements in Part 2 of the SOCI Act;
- Organisations must notify the Australian Signals Directorate ("**ASD**") of actual or imminent cyber security incidents with an actual or likely relevant impact within 72 hours of the organisation becoming aware, in accordance with the requirements set out in Part 2B of the SOCI Act; and
- Organisations must implement and comply with a "risk management program", in accordance with the requirements in Part 2A of the SOCI Act and the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023.

Generally, organisations to whom the SOCI Act applies or those that provide services to relevant organisations should ensure that any terms and conditions deal with compliance with the obligations under the SOCI Act.

Consumer Data Right

The Commonwealth Government is in the implementation phases of the Consumer Data Right (“**CDR**”) following a number of policy reviews including the Productivity Commission's "Data Availability and Use" report and the "Review into Open Banking in Australia".

The CDR allows a consumer to obtain certain data held about that consumer by a third party and require data to be given to accredited third parties for certain purposes. By requiring businesses to provide public access to information on specified products they have on offer, it is intended that consumers' ability to compare and switch between products and services will be improved, as well as encouraging competition between service providers, which could lead to better prices for customers and more innovative products and services. In this way, the CDR provides a mechanism for accessing a broader range of information within designated sectors than is provided for by APP 12 in the Privacy Act, given it applies not only to data about individual consumers but also to business consumers and related products.

The CDR rules have been implemented in respect of the banking and energy sector in Australia. The non-bank lending sector is the next to be added to the CDR. Other sectors across the economy will be added to the CDR over time.

The CDR regime addresses competition, consumer, privacy and confidentiality issues. As such, it is regulated by the Australian Competition and Consumer Commission as well as the OAIC.

DEFINITIONS

Definition of personal data

Personal data (referred to as "personal information" in Australia) means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in material form or not.

The Privacy Act currently contains an exemption for “employee records”, such that any records containing personal information which an employer makes in connection with a current or former employment relationship are exempt from the Privacy Act. However there are some further carve outs to this (for example, the exemption does not apply to contractors or unsuccessful applicants), and it is widely anticipated that the employee records exemption will be removed from the Privacy Act as a result of the ongoing review of the Privacy Act (see Enforcement).

Definition of sensitive personal data

Sensitive personal data (referred to as "sensitive information" in Australia) means information or an opinion about:

- Racial or ethnic origin;
- Political opinions;
- Membership of a political association;
- Religious beliefs or affiliations;
- Philosophical beliefs;
- Membership of a professional or trade association;
- Membership of a trade union;
- Sexual orientation or practices;
- Criminal record that is also personal information;
- Health information about an individual;

- Genetic information about an individual that is not otherwise health information;
- Biometric information that is to be used for the purpose of automated biometric identification or verification; and / or
- Biometric templates.

NATIONAL DATA PROTECTION AUTHORITY

The Information Commissioner, under the Office of the Australian Information Commissioner ("**OAIC**") is the national data protection regulator responsible for Privacy Act oversight.

175 Pitt Street
Sydney NSW 2000

T 1300 363 992

F +61 2 9284 9666

REGISTRATION

There is no registration requirement in Australia for data controllers or data processing activities. Under the Privacy Act, organizations are not required to notify the Information Commissioner of any processing of personal information.

DATA PROTECTION OFFICERS

Organizations are not required to appoint a data protection officer. However, the Information Commissioner has issued guidance recommending that organizations appoint a data protection officer as good practice.

COLLECTION & PROCESSING

Organizations may not collect personal information unless the information is reasonably necessary for one or more of its business functions or activities.

Under the Privacy Act, organizations must take reasonable steps to ensure that personal information collected is accurate and up-to-date.

At or before the time organizations collect personal information, or as soon as practicable afterwards, they must take reasonable steps to provide individuals with notice of:

- The Organization’s identity and contact information;
- Why it is collecting (or how it will use the) information about the individual;
- The entities or types of entities to which it might give the personal information;
- Any law requiring the collection of personal information;
- The main consequences (if any) for the individual if all or part of the information is not provided;
- The fact that the organization’s privacy policy contains information about how the individual may access and seek correction of their personal information, how they may make a complaint about a breach of the APPs and how the organization will deal with such complaint; and
- Whether the organization is likely to disclose their personal information to overseas recipients and, if so, the countries in which such recipients are likely to be located.

Organizations should comply with these notification requirements by preparing a “collection statement” or “privacy notice” for each significant collection of personal information, and providing this to individuals prior to collecting their personal information.

This notification requirement applies in addition to the requirement for organisations to maintain a broader privacy policy, which details the general personal information handling processes of the organisation. APP 1 lists the information which is required to be included in a privacy policy.

In practice, a major Privacy Act compliance issue often arises because organizations fail to recognize that the mandatory notice requirements outlined above also apply to any personal information collected from a third party. Organizations must provide individuals with required notice on receipt of personal information from a third party, even though they did not collect personal information directly from the individual. Unlike Europe, Australian privacy law does not distinguish between "data processors" and "data controllers".

Organizations must not use or disclose personal information about an individual unless one or more of the following applies:

- The personal information was collected for that purpose (the primary purpose) or a different (secondary) purpose which is related to (and, in the case of sensitive information, directly related to) the primary purpose of collection and the individual would reasonably expect the organization to use or disclose the information for that secondary purpose.
- The individual consents.
- The information is not sensitive information and disclosure is for direct marketing and it is impracticable to seek the individual’s consent and (among other things) the individual is told that they can opt out of receiving marketing from the organization.
- A "permitted general situation" or "permitted health situation" exists; for example, the entity has reason to suspect that unlawful activity relating to the entity's functions has been engaged in, or there is a serious threat to the health and safety of an individual or the public.
- It is required or authorized by law or on behalf of an enforcement agency.

In the case of use and disclosure for the purpose of direct marketing, organizations are required to ensure that:

- Each direct marketing communication provides a simple means by which the individual can opt out
- The individual has not previously requested to opt out of receiving direct marketing communications

The above direct marketing requirements apply to all forms of direct marketing. Additionally, specific requirements for commercial electronic messaging are outlined in Electronic Marketing.

The Privacy Act affords additional protections when processing involves sensitive information. Organizations are prohibited from collecting sensitive information from an individual unless certain limited requirements are met, including one or more of the following:

- The individual has consented to the collection and the collection of the sensitive information is reasonably necessary for one or more of the entity's functions or activities.
- Collection is required or authorized by law or a court / tribunal order.
- A "permitted general situation" or "permitted health situation" exists; for example, the entity has reason to suspect that unlawful activity relating to the entity's functions has been engaged in, or there is a serious threat to the health and safety of an individual or the public.
- The entity is an enforcement body and the collection is reasonably necessary for that entity's functions or activities.
- The entity is a nonprofit organization and the information relates to the activities of the organization and solely to the members of the organization (or to individuals who have regular contact with the organization relating to its activities).

Organizations must provide individuals with access to their personal information held by the organization upon an individual’s request. Additionally, individuals have a right to correct inaccurate, out-of-date, and irrelevant personal information held by an organization. Under certain circumstances, the organization may limit the extent to which it provides an

individual with access or correction rights, including in emergency situations, specified business imperatives, and law enforcement or other public interests.

Further, organizations must provide individuals with the option to not identify themselves, or use a pseudonym, when dealing with the organization, unless it is impractical to do so or the organization is required or authorized by law to deal with identified individuals.

TRANSFER

Unless certain limited exemptions under the Privacy Act apply, personal information may only be disclosed to an organization outside of Australia where the entity has taken reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the personal information. The disclosing / transferring entity will generally remain liable for any act(s) done or omissions by that overseas recipient that would, if done by the disclosing organization in Australia, constitute a breach of the APPs. However, this provision will not apply where any of the following apply:

- The organization reasonably believes that the recipient of the information is subject to a law or binding scheme which effectively provides for a level of protection that is at least substantially similar to the Privacy Act, including as to access to mechanisms by the individual to take action to enforce the protections of that law or binding scheme. There can be no reliance on contractual provisions requiring the overseas entity to comply with the APPs to avoid ongoing liability (although the use of appropriate contractual provisions is a step towards ensuring compliance with the 'reasonable steps' requirement).
- The individual consents to the transfer. However, under the Privacy Act the organization must, prior to receiving consent, expressly inform the individual that if he or she consents to the overseas disclosure of the information the organization will not be required to take reasonable steps to ensure the overseas recipient does not breach the APPs.
- A "permitted general situation" applies.
- The disclosure is required or authorized by law or a court / tribunal order.

SECURITY

An organization must have appropriate security measures in place (i.e. take reasonable steps) to protect any personal information it retains from misuse and loss and from unauthorized access, modification or disclosure. The Information Commissioner has issued detailed guidance on what it considers to be reasonable steps in the context of security of personal information, which we recommend be reviewed and implemented. Depending on the organization, and how and by which government agency it is regulated, as noted above specific requirements or expectations may also exist and with which organizations should be familiar. An organization must also take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for the purpose(s) for which it was collected.

BREACH NOTIFICATION

Entities with obligations to comply with the Privacy Act must comply with the mandatory data breach notification regime under the Privacy Act.

The mandatory data breach notification includes data breaches that relate to:

- Personal information
- Credit reporting information
- Credit eligibility information
- Tax file numbers

In summary, the regime requires organizations to notify the OAIC and affected individuals of "eligible data breaches" (in accordance with the required contents of a notice). Where it is not practicable to notify the affected individuals individually, an organization that has suffered an eligible data breach must make a public statement on its website containing certain information as required under the Privacy Act, and take reasonable steps to publicise the contents of the statement.

An "eligible data breach" occurs when the following conditions are satisfied in relation to personal information, credit reporting information, credit eligibility information or tax file information:

All of the following conditions are satisfied:

- There is unauthorized access to, or unauthorized disclosure of, or loss of the information;
- A reasonable person would conclude that the access or disclosure, or loss would be likely to result in serious harm to any of the individuals to which the information relates; and
- Prevention of the risk of serious harm through remedial action has not been successful.

While "serious" harm is not defined in the legislation, the OAIC has released guidance on how serious harm may be interpreted and assessed by organizations. There are a number of key criteria to examine when determining if "serious" harm is likely to result from a breach which should be assessed holistically and take into account: the kinds of information, sensitivity, security measures protecting the information, the nature of the harm (i.e. physical, psychological, emotional, financial or reputational harm) and the kind(s) of person(s) who may obtain the information.

The regime also imposes obligations on organizations to assess within 30 calendar days whether an eligible data breach has occurred where the organization suspects (on reasonable grounds) that an eligible data breach has occurred, but that suspicion does not amount to reasonable grounds to believe that an eligible data breach has occurred.

There are various exceptions to the requirement to notify affected individuals and / or the OAIC of a data breach notification including in instances where law enforcement related activities are being carried out or where there is a written declaration by the Information Commissioner.

The introduction of the regime has resulted in many organizations requiring detailed contractual obligations with third party suppliers in relation to cybersecurity and the protection of personal information of their customers / clients. Complimenting this regime, the OAIC has also released several guidance notes relating to the regime which include topics such as the security of personal information and whilst these are not legally binding, they are considered industry best practice.

Further, organizations may have additional obligations to notify other regulators of data breaches in certain circumstances including under the Prudential Standard CPS 234 Information Security ("**CPS 234**") which aims to strengthen APRA-regulated entities' resilience against information security incidents (including cyberattacks), and their ability to respond swiftly and effectively in the event of a breach. CPS 234 applies to all APRA-regulated entities who among other things, are required to notify APRA within 72 hours "after becoming aware" of an information security incident and no later than 10 business days after "it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner".

ENFORCEMENT

The Information Commissioner is responsible for the enforcement of the Privacy Act and will investigate an act or practice if the act or practice may be an interference with the privacy of an individual and a complaint about the act or practice has been made. Generally, the Information Commissioner prefers mediated outcomes between the complainant and the relevant organization. Importantly, where the Information Commissioner undertakes an investigation of a complaint which is not settled, it is required to ensure that the results of that investigation are publicly available. Currently, this is undertaken by disclosure through the OAIC website of the entire investigation report.

The Information Commissioner may also investigate any "interferences with the privacy of an individual" (i.e. any breaches of the APPs) on its own initiative (i.e. where no complaint has been made) and the same remedies as below are available. With a number of large scale, high profile data breaches occurring in Australia recently, the Information Commissioner appears to be adopting a more proactive and more publicised approach to investigation and enforcement action, and it seems likely that the review and likely revision of the Privacy Act will strengthen the Information Commissioner's powers with respect to investigation and enforcement.

After investigating a complaint, the Information Commissioner may dismiss the complaint or find the complaint substantiated and make declarations that the organization rectify its conduct or that the organization redress any loss or damage suffered by the complainant (which can include non-pecuniary loss such as awards for stress and / or humiliation). The maximum penalties that may be sought by the Information Commissioner and imposed by the Courts for serious or repeated interferences with the privacy of individuals were increased significantly to the greater of (i) AUD50M, (ii) three times the benefit of a contravention, or (iii) (where the benefit cannot be determined) 30% of domestic turnover.

ELECTRONIC MARKETING

The sending of electronic marketing (referred to as "commercial electronic messages" in Australia) is regulated under the Spam Act 2003 (*Cth*) (“**Spam Act**”) and enforced by the Australian Communications and Media Authority.

Under the Spam Act, a commercial electronic message (which includes emails and SMS's sent for marketing purposes) must not be sent without the prior opt-in consent of the recipient.

In addition, each electronic message (which the recipient has consented to receive) must identify the sender and contain a functional unsubscribe facility to enable the recipient to opt out of receiving future electronic marketing. Requests to unsubscribe must be processed within 5 business days.

A failure to comply with the Spam Act (including unsubscribing a recipient that uses the unsubscribe facility) may have costly consequences, with repeat offenders facing penalties of up to AU$2.2 million per day.

ONLINE PRIVACY

There are no laws or regulations in Australia specifically relating to online privacy, beyond the application of the Privacy Act, the Spam Act and State and Territory privacy laws relating to online / e-privacy, and other specific laws regarding the collection of location and traffic data. Specifically, the are no specific legal requirements regarding the use of cookies (or any similar technologies). If the cookies or other similar technologies collect personal information of a user the organization must comply with the Privacy Act in respect of collection, use, disclosure and storage of such personal information. App developers must also ensure that the collection of customers' personal information complies with the Privacy Act and the Information Commissioner has released detailed guidance on this.

KEY CONTACTS

Nicholas Boyle
Partner
T +61 2 9286 8479
nicholas.boyle@dlapiper.com

Sarah Birkett
Special Counsel
DLA Piper Australia
T +61 3 9274 5464
sarah.birkett@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

AUSTRIA

Last modified 27 December 2022

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

In Austria, the laws concerning the implementation of the GDPR have been adopted gradually. In summer 2017, the existing Data Protection Act 2000 (*Datenschutzgesetz 2000*) was amended by the Data Protection Amendment Act 2018 (*Datenschutz-Anpassungsgesetz 2018*) which constituted the first implementation of various regulations related to GDPR, and was intended to enter into force simultaneously with GDPR. The 'Data Protection Act' (*Datenschutzgesetz, DSG)* has considerably amended the Data Protection Act 2000. In addition to the GDPR, it is now the central piece of legislation in Austria regulating data privacy.

The Privacy Deregulation Act 2018 (*Datenschutz-Deregulierungs-Gesetz 2018*) further amended the DSG. The DSG, as amended by the Privacy Deregulation Act 2018, came into force on May 25, 2018 and is now the applicable regulation in Austria. The DSG also includes the implementation of the Directive (EU) 2016/680.

In addition to the DSG, further amendments to other statutory laws were adopted in order to implement the GDPR (mostly to adapt to the terminology of the GDPR). These amendments were included in the General Data Protection Adjustment Act (*Materien-Datenschutz-Anpassungsgesetz 2018*) and the research-sector specific Data Protection Adjustment Act – Science and Research (*Datenschutz- Anpassungsgesetz 2018 – Wissenschaft und Forschung – WFDSAG 2018*). Further amendments in other laws have been made by the Second General Data Protection

Adjustment Act, which was passed in June 2018 and applies retroactively. Finally, ordinances were also passed regulating respectively the cases where a data privacy impact assessment is obligatory (the Obligatory DPIA Ordinance - *DSFA-V*) and the exemptions from the obligation to conduct a data privacy impact assessment (the DPIA Exemptions Ordinance - DSFA-AV).

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly referred to in Recital 30, with IP addresses, cookies and RFID tags listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR concerns the " **processing**" of personal data. Processing has a broad meaning, and includes any set of operations performed on data, including mere storage, hosting, consultation or deletion.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor " *processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to former legislation, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The DSG does not include any additional definitions or derogations to the GDPR. However, Section 1 DSG, which provides a constitutional (human) right to data privacy, does not use the definition of "data subject" of the GDPR, but rather uses the term "everyone" which is currently interpreted to include legal entities and other organizations too. Consequently, the constitutional (human) right to data privacy, as well as some basic data subject rights, as regulated in Section 1 DSG, also apply to legal entities and other organizations.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is conducted by data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (successor of the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR establishes the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Austrian Data Protection Authority (*Österreichische Datenschutzbehörde*) can be contacted as follows:

Österreichische Datenschutzbehörde
Barichgasse 40-42 1030 Vienna
Austria / Europe
Phone number: +43 1 52 152-0
E-Mail: dsb@dsb.gv.at

If possible, the Austrian Data Protection Authority prefers to communicate via email.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if one of the following conditions are met:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;

- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

The DSG contains in its Section 5 some additional regulation in respect to the rights and obligations of the DPO. Thereunder, the DPO and all persons working for the DPO are obliged to retain confidentiality regarding the identity of the persons that have approached the data protection officer as well as regarding all the circumstances that could reveal the identity of such persons.

Under certain circumstances, the DPO and their assistant personnel have the right to refuse testimony regarding the data obtained in their capacity as data protection officer, if a person employed in a position subject to the data protection officer's supervision is entitled to such right and to the extent that person has exercised such right. All files and other documents of the data protection officer which are subject to this statutory right to remain silent in the aforementioned extent cannot be lawfully seized.

Further regulations in Section 5 concern the DPOs of public organizations.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core principle of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance, potentially for years after a particular decision regarding processing of personal data. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;

- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce national legislation regarding processing of genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by national legislation (Article 10).

Section 4 Para 3 DSG regulates the processing of data regarding actions punishable under criminal or administrative law, criminal convictions or suspected criminal actions.

Processing must (i) be based on an explicit legal authorization or obligation to process such data or (ii) be justified by a statutory duty of care or legitimate interests pursuant to Article 6 (1) lit f GDPR, and be carried out in a manner ensuring to protect the data subjects interests set out in the GDPR and the DSG.

For example, legitimate interest may be established in recruitment processes for trustworthy personnel.

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Austrian DSG imposes further obligations upon controllers and processors. Pursuant to Section 6, all employees, agents or contractors of a controller or a processor who have access to personal data must be contractually obliged to transfer personal data only after receiving an adequate and documented instruction by their employer (confidentiality

obligation). All employees, agents or contractors of a controller or a processor must be subject to confidentiality undertakings or professional or statutory obligations of confidentiality. Measures must be taken to ensure that all employees, agents or contractors of a controller or a processor are bound by the aforementioned undertakings and/or obligations of confidentiality even after the termination of their respective contract, regardless of the cause or form thereof.

CCTV, or rather more broadly processing of images made in public or private spaces, including related sound recordings, are subject to further regulation and requirements pursuant to Sections 12 and 13 DSG. This provision provides limitations regarding the lawfulness of such processing as compared to Art 6 GDPR, as processing of image data is only permissible in the following cases:

- processing is necessary in order to protect the vital interests of the data subject
- the data subject has given their consent
- the processing is required or permitted by specific statutory law, or
- the interests of the data controller override the interests of the data subjects in the specific case, and the processing is proportionate

Overriding legitimate interests are assumed by the law in some cases listed as examples, such as preventive protection of property or persons on private properties or publicly accessible spaces controller by the data controller.

The capturing of images / CCTV is always prohibited in the following cases:

- processing of images capturing persons in their personal area of life without their express consent
- processing of CCTV images for the purpose of employee monitoring
- the automated comparison of personal data obtained by means of capturing images / CCTV without explicit consent and for the creation of personality profiles with other personal data, or
- the evaluation of personal data obtained by means of image capturing on the basis of special categories of personal data (Art. 9 GDPR) as a selection criterion

In early 2020, the Austrian Data Protection Authority has published a non-binding opinion, referring to two decisions of the Federal Administrative Court, and stating that Sections 12 and 13 DSG are not in line with the GDPR and shall therefore no longer be applied. The Authority shall assess CCTV data processings exclusively on the basis of the GDPR. However, the contents of the Sections 12 and 13 DSG are still practically used as criteria for assessment of the lawfulness of the processing.

Other additional regulations for processing of data include:

- regulation relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Section 7), which allows processing of such data if they are publicly accessible, have been collected lawfully for other research purposes or other lawful purposes, or are pseudonymized; other data may only be processed to the extent there are specific statutory regulations, the data subjects have given their consent or the Data Protection Authority has approved the processing
- further regulation regarding the processing of data for purposes pursuant to Art 89(1) GDPR, most notably for research purposes, included in the Act on Research Organisation (*Forschungsorganisationsgesetz* - FOG); this regulation includes provisions which lessen to some extent the requirements for processing of special categories of data, including in particular the concept of "broad consent", and limit the rights of data subjects in this respect
- regulation relating to the processing of addresses for informing or sending questionnaires to data subjects (Section 8), which in principle requires consent for such processing, but also provides some derogations
- regulation regarding data processing in cases of catastrophes (Section 10)

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules and standard contractual clauses. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defense of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

Section 13 DSG imposes further obligations on Controllers in regard to CCTV and / or processing of captured images pursuant to Section 12 DSG. The controller needs to secure the access to the CCTV / captured images in a way that makes any access and / or subsequent alteration of captured images by an unauthorized third party impossible.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, they are required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. The Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. Under EU case-law regarding competition, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. It is not yet clear whether this will translate directly to GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy broad investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR provides for specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" because of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss. These claims can be made at any competent court.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Furthermore, individuals may lodge a complaint to a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

In Austria, the Austrian Data Protection Authority is responsible for the enforcement of the GDPR. Pursuant to Section 11 DSG, the Austrian Data Protection Authority is obliged to impose administrative fines pursuant to the Article 83 GDPR in an adequate way. The Authority should in particular also apply the measures pursuant to Art 58 GDPR in case of first time breaches, in particular the possibility to issue warnings instead of imposing fines.

The fines under the GDPR are imposed under Austrian administrative criminal law. The Austrian administrative criminal law in general does not allow authorities to impose fines against a legal entity, but provides only for the liability of natural persons; in cases where violations are committed by a legal entity, the liable persons are either statutory representatives (directors) or persons appointed as responsible persons for adherence with specific administrative laws. However, the DSG provides a possibility to impose fines against legal entities, in the following cases:

- A violation of GDPR or DSG is committed by a natural person who has power (1) to represent the legal entity or to make decisions on behalf of the legal entity; or (2) has supervisory powers in the legal entity and has committed this offence either alone or as a part of an organ of the legal entity (*eg*, management board)

- An employee of the legal entity violates the provisions of GDPR or DSG and the violation was possible due to insufficient supervision or control by a person by a natural person that has power to (1) represent the legal entity; (2) or to make decisions on the behalf of the legal entity; or (3) has supervisory powers in the legal entity, provided the violation is not subject to criminal law.

The possibility to impose fines against a legal entity or a responsible natural person, as appropriate. If the fine is imposed against a legal entity, the Authority is required to identify a particular natural person whose violations are to be attributed to said entity; the responsible natural person may not be fined for the same breach.

Public bodies cannot be fined for violations of GDPR or DSG.

ELECTRONIC MARKETING

The GDPR applies to most electronic marketing activities, as these will involve use of personal data (eg, an email address which includes the recipient's name). The most relevant legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR apply, and marketing consent forms will need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State, provides for specific rules on electronic marketing (including circumstances in which consent must be obtained). The ePrivacy Directive is yet to be replaced by a Regulation. However, it is currently uncertain when this is going to happen. In the meantime, Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The GDPR or DSG do not specifically address (electronic) marketing, however, the use of personal data for marketing purposes is clearly within their scope. It is arguable that the processing of personal data of the existing customers within the scope of the business is permissible for marketing purposes, and this has become common practice in Austria. For persons who are not yet customers, the consent of the data subjects is generally required.

Electronic marketing is also regulated by the Austrian Telecommunications Act (*Telekommunikationsgesetz* 2021, 'TKG'). Pursuant to the TKG the sending of electronic messages without prior consent of the recipient is unlawful, if the sending is for direct marketing purposes. No consent is required if the data has been obtained in the course of the sale of goods or provision of services, occurs for the same or similar goods or services, the recipient is able to decline easily and with no costs for the use of his or her personal data and the recipient has not previously declared, by requesting to be entered on to the relevant list (maintained by the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR)), that they do not want to be contacted.

The GDPR implementation Acts do not provide any amendments or derogations in respect of electronic marketing. However, electronic marketing was and still is separately regulated in Austria in the Telecommunications Act (*Telekommunikationsgesetz* 2021, TKG), Section 174, which implements the ePrivacy Directive.

Pursuant to the TKG the sending of electronic messages without prior consent of the recipient is unlawful insofar as the message is sent for direct marketing purposes. Explicit consent is not required where (1) the data have been obtained in

the context of the sale of goods or provision of services; (2) the electronic marketing concerns same or similar goods or services of the sender; (3), the recipient is able to decline easily and with no costs for the use of his or her personal data for electronic marketing, both when the data are collected as well as with each message received ('opt-out'), and the recipient has not previously declared, by requesting to be entered on to the relevant lists (the "Robinson lists", maintained by the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) and the Austrian Chamber of Commerce (WKO)), that he or she does not want to be contacted.

ONLINE PRIVACY

Online privacy is specifically regulated by the TKG.

Traffic data

Traffic Data held by communications services providers (CSPs) must be erased or anonymized when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained for purposes of invoicing the services. In such a case, if the invoice has been paid and no appeal has been lodged with the CSP within three months the Traffic Data must be erased or anonymized.

Location data

Location Data may only be processed for emergency services and with consent of the user. Even in case of consent, the user must be able to prohibit the processing by simple means, for free of charge and for a certain time period.

Cookie compliance

The relevant section of the TKG stipulates that a user must give informed consent for the storage of personal data, which includes a cookie. The user has to be aware of the fact that consent for the storage or processing of personal data is given, as well as the details of the data to be stored or processed, and has to agree actively. Therefore obtaining consent via some form of pop-up or click through agreement seems advisable. Consent by way of browser settings, or a pre-selected checkbox etc. is probably not sufficient in this respect.

If for technical reasons the short term storage of content data is necessary, such data must be deleted immediately thereafter.

Online privacy is still specifically regulated by the TKG, and the GDPR implementation acts have introduced only minor amendments thereto. There are no regulations regarding online privacy in the DSG itself.

Media privilege

In an effort to balance freedom of speech and freedom of information publishers as well as owners and employees of media outlets are granted privileges regarding the processing of data for journalistic purposes (Section 9 DSG). Certain Chapters of the GDPR are not applicable to such processings, specifically:

- Chapter II (Principles);
- Chapter III (Rights of the data subject);
- Chapter IV (Controller and Processor);
- Chapter V (Transfers of personal data to third countries or international organizations);
- Chapter VI (Independent supervisory authorities);
- Chapter VII (Cooperation and consistency); and
- Chapter IX (Provisions relating to specific processing situations).

The same exceptions (with the slight difference of Article 5 of Chapter II remaining applicable) are stipulated if data is processed for scientific, artistic or literary purposes.

KEY CONTACTS

Sabine Fehringer
Partner
T +43 1 531 78 1460
sabine.fehringer@dlapiper.com

Stefan Panic
Counsel
T +43 531 78 1034
stefan.panic@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

AZERBAIJAN

Last modified 15 February 2022

LAW

Law on Personal Information dated 11 May 2010.

DEFINITIONS

Definition of Personal Data

Any information allowing to identify a person, directly or indirectly, is considered personal data.

Definition of Sensitive Personal Data

Personal data of special category includes information relating to race or nationality of an individual, his/her family life, religion and belief, health or conviction.

NATIONAL DATA PROTECTION AUTHORITY

The major regulator/enforcement authority (DPA) is the Ministry of Digital Development and Transport.

In addition, the other designated state authorities which are vested in powers to enforce applicable data protection/privacy laws, within the scope of their competences, include the Ministry of Internal Affairs, the Ministry of Justice, the State Security Service, and the Special State Protection Service.

REGISTRATION

Information systems of personal data must be registered with the DPA. There are also certain exemptions from such registration requirement.

DATA PROTECTION OFFICERS

The DPA, through its officers, may demand elimination of violations of statutory requirements by legal entities and individuals, also take necessary actions for holding accountable persons who breached the statutory requirements regarding collection, processing and protection of personal data.

COLLECTION & PROCESSING

Collection and processing of personal data can be implemented either with obtaining a prior consent of a data subject or when the data is of open category (i.e. non-confidential).

TRANSFER

Transfer of personal data can be performed with a prior written consent of a data subject, unless the data is of open category.

SECURITY

Adequate level of protection of personal data should be provided by owners of operators of personal data.

BREACH NOTIFICATION

There is no specific requirement as to notification of the DPA by the owner or operator of personal data about breach.

ENFORCEMENT

If the rights of a data subject are breached as a result of the illegal collection and processing of personal data, inadequate protection of such data, or non-compliance with the statutory requirements, the data subject may claim for compensation of material and moral damages sustained by him/her through the local court.

ELECTRONIC MARKETING

No consent of a recipient is required for e-mail marketing, provided only that service providers must establish a registration system for persons who wish to opt out from receiving marketing materials, and comply with such system.

ONLINE PRIVACY

There are no rules directly regulating use of cookies in Azerbaijani legislation. However, if cookies contain any personal data, the Azerbaijani data protection rules will apply as to the use of such cookies.

If a data subject cannot be identified just based on location data, it would unlikely be deemed as personal data, falling outside the scope of personal data protection related requirements.

KEY CONTACTS

MGB Law Offices
mgb-law.com/

Ismail Askerov
Senior Partner
MGB Law Offices
T +99412 493 6669
ismail.askerov@mgb-law.com

Lala Hasanova
Senior Associate
MGB Law Offices
T +99412 493 6669
lala.hasanova@mgb-law.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BAHAMAS

Last modified 26 January 2023

LAW

Data Protection (Privacy of Personal Information) Act **(“DPA”).**

Note that in October 2023, the Governor General of The Bahamas, in the customary Speech from the Throne meant to present the Government of The Bahamas’ legislative and policy agenda, declared the government’s intention to enact new data protection legislation. As of January 2024, there has been no formal disclosure of specific details about the extent of reform that may be seen or a timeline for which a Bill may be laid before Parliament.

DEFINITIONS

Definition of Personal Data

Section 2 DPA defines ‘personal data’ as data relating to a living individual who can be identified either from the data or from the data in conjunction with other information in the possession of the data controller.

Definition of Sensitive Personal Data

‘Sensitive personal data’ is further defined in Section 2 DPA as personal data relating to: racial origin; political opinions or religious or other beliefs; physical or mental health (other than any such data reasonably kept by them in relation to the physical or mental health of their employees in the ordinary course of personnel administration and not used or disclosed for any other person); trade union involvement or activities; sexual life; or criminal convictions, the commission or alleged commission of any offence, or any proceedings for any offence committed, the disposal of such proceedings or the sentence of any court in such proceedings.

It should be noted that although sensitive personal data (‘**SPD**’) is distinguished from personal data under DPA in its specificity of certain categories of data, SPD does not otherwise receive any special treatment compared to general personal data. While DPA provides that the relevant Minister responsible for data protection may create regulations that would provide safeguards for such data under the Act, such a regulation has never materialized.

NATIONAL DATA PROTECTION AUTHORITY

Section 14 DPA establishes a Data Protection Commissioner (‘**DPC**’), a corporation sole, that is tasked with the enforcement of the provisions of DPA. The DPC operates from the Office of the Data Protection Commissioner which would the Bahamian equivalent of a national data protection authority as seen in other jurisdictions.

REGISTRATION

There is no obligation under DPA to register with the Office of the Data Protection Commissioner as a data controller (or data processor).

DATA PROTECTION OFFICERS

There is no statutory duty to appoint a Data Protection Officer under DPA.

COLLECTION & PROCESSING

DPA in The Bahamas has only limited extraterritorial effect (as it concerns data controllers). Per Section 4(1) of DPA, the Act only applies to: data controllers established in The Bahamas (where the data is processed in the context of the local establishment); and data controllers established outside The Bahamas that use equipment in The Bahamas for processing data (other than for transit through The Bahamas).

In the above context, an ‘established’ data controller can be any of the following (in accordance with Section 4(3) of DPA): an individual ordinarily resident in The Bahamas; a body incorporated or registered under Bahamian law; a partnership or other unincorporated association formed under Bahamian law; and any person that does not fall into any of the foregoing categories but maintains an office, branch or agency in The Bahamas through which they carry on a business activity or regular practice. It can be seen, therefore, that a nexus to The Bahamas of the kind described above must be established for DPA to apply outside the jurisdiction.

Data controllers are defined in Section 2 DPA as a person who, alone or with others, determines the purposes for which and the manner in which any personal data are, or are to be processed. Data controllers owe a statutory duty of care to data subjects pursuant to Section 12(1) as it regards the collection by him of personal data or information intended for inclusion in such data or his dealing with such data. Further, Section 12(2) provides that data controllers must use contractual or other legal means to provide a ‘comparable’ level of protection from any third party to whom he discloses information for the purpose of data processing.

Data controllers, under Sections 6(1), must abide by several core duties as it relates that the collection, processing, keeping, use and disclosure of data of data subjects, namely, to ensure:

- The data or information constituting the data has been collected by means which are lawful and fair in the circumstances of the case (e.g., data subjects should not be deceived or misled as to the purpose(s) for which the data is being processed or collected – and the use of such data should not cause damage or distress to the data subject);
- The data is accurate and kept up to date where necessary (except in the case of data back-up);
- The data is only kept only for one or more specified or lawful purpose(s);
- The data is not used or disclosed in a manner which is incompatible with that/those purpose(s);
- The data collected is adequate, relevant and not excessive in relation to that purpose or purposes;
- The data is not kept for a period longer than necessary for the purpose(s) for which it was collected (except in cases where personal data needs to be kept for historical, statistical or research purposes);
- There are appropriate security measures in place to prevent unauthorised access to, or alteration, disclosure or destruction of data and against its accidental loss or destruction.

TRANSFER

Section 17 DPA speaks to the international transfer of data. Under Section 17(1) the DPC may prohibit the transfer of personal data from The Bahamas to a place outside The Bahamas in cases where there is a failure to provide protection either by contract or otherwise equivalent to that provided under DPA, subject to certain exceptions. In arriving at a determination to prohibit the international transfer of data, the DPC must consider whether such a transfer would cause damage or distress to any person and consider the desirability of the transfer. Pursuant to Section 17(8) however, data constituting data required or authorized to be transferred under another enactment; or data that is required by any convention or other instrument imposing an international obligation on The Bahamas; or otherwise, data that a data subject has consented to having transferred, will not apply under Section 17.

SECURITY

As mentioned previously, Section 6(1)(d) provides that data controllers must ensure that appropriate security measures are taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. In practice, appropriate security measures typically mean ‘industry-standard’ (particularly for institutions that store SPD, e.g. law firms, hospitals, banks, insurance companies, etc).

BREACH NOTIFICATION

There is no breach notification obligation under the provisions of DPA.

ENFORCEMENT

The DPC of The Bahamas is largely responsible for the enforcement of data protection in the jurisdiction. Section 15(1) states that the DPC may investigate or cause to be investigated whether any of the provisions of DPA have been contravened by a data controller or a data processor in relation to an individual when an individual has complained of a contravention of any DPA provisions or where he may otherwise be of the opinion that a contravention make have occurred. Enforcement measures the DPC can utilize include enforcement notices (Section 16 DPA), prohibition notices (Section 17 DPA), information notices (Section 18 DPA), and in rare instances bringing and prosecuting summary offences under DPA (Section 28 DPA).

Aside from its statutory functions, the DPC is also tasked with educating the public of data protection issues and trends and providing assistance in data breach remediation.

In accordance with Section 29(1) DPA, penalties for a person guilty of an offence under DPA are liable on summary conviction to a fine not exceeding $2,000.00 Bahamian Dollars; or on conviction on information, to a fine not exceeding $100,000.00 Bahamian Dollars. Further, Section 29(2) provides that where a person is convicted of a DPA offence, the court may also order that any data material which appears to the court to be connected with the commission of the offence to be forfeited or destroyed and any (relevant) data to be erased.

ELECTRONIC MARKETING

Data subjects have the right to prohibit processing for the purposes of direct marketing by way of Section 11 DPA. Though DPA provides that ‘direct marketing’ includes direct mailing, it also applies by extension to electronic marketing and newsletters. In order to prohibit such processing a data subject may make a written request to the data controller to cease using any data that has been kept for the purpose of direct marketing. The data controller then has no more than forty days to either erase or cease using the said data and notify the data subject in writing accordingly.

ONLINE PRIVACY

Outside of the current provisions of DPA and legislation governing law enforcement access to one’s computing devices and encrypted data (e.g. the Interception of Communications Act, Computer Misuse Act, National Crime Intelligence Agency Act etc.), online privacy is largely unregulated and there are no specific laws aimed at the use of cookies or the collection of location data.

Under the Electronic Communications and Transactions Act (‘**ECTA**’), however, Section 20 provides for online intermediary a procedure for ‘dealing with unlawful, defamatory, etc. information’. An intermediary is defined under Section 2 ECTA as, in the context of an electronic communication, a person including a host on behalf of another person who sends, receives or stores either temporary or permanently that electronic communication or provides related services with respect to that electronic communication. Section 20(1) states that where an intermediary has actual knowledge that information in an electronic communication gives rise to civil or criminal liability, then as soon as possible the intermediary should remove the information from any information processing system within the intermediary’s control and cease to provide or offer services in respect of that information and notify the police of the any relevant facts and of the identity of the person from whom the intermediary was supplying services in respect of the information, if the identity of that person is known to the intermediary. Similarly, Section 20(2) states that if an intermediary is aware of facts or circumstances from which the *likelihood* of civil or criminal liability in respect of the information in an electronic communication ought reasonably to have been known should, as

soon as practicable, follow any relevant procedure set out in any code of conduct that may be applicable to the intermediary under the Act or notify the police and relevant Minister responsible for electronic communications. The Minister may then direct the intermediary to remove the electronic communication from any information processing system within the control of the intermediary and cease to provide services to the person to whom the intermediary was supplying services in respect of that electronic communication. It can be argued that these provisions give intermediaries (e.g. telecommunications providers) facilitating communications between end users’ communications broad powers to potentially cease services or effectively censor electronic communications they deem objectionable on the grounds that civil or criminal liability could likely arise without any liability arising provided the action is made in good faith.

KEY CONTACTS

GrahamThompson
grahamthompson.com/

Sean G. McWeeney Jr.
Associate
GrahamThompson
T +1 (242) 322-4130
sgm@gtclaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BAHRAIN

Last modified 17 January 2024

LAW

Bahrain enacted Law No. 30 of 2018 with respect to Personal Data Protection ("**PDPL**") on July 12, 2018. The PDPL is the main data protection regulation in Bahrain. The PDPL came into force on August 1, 2019, and supersedes any law with contradictory provisions. On March 17, 2022, the Personal Data Protection Authority ("**Authority**") has issued 10 ministerial resolutions supplementing the PDPL ("**Resolutions**"). The Resolutions cover the following:

1. duties of the Data Protection Officer and related fees;
2. technical and organisational measures;
3. notification procedures;
4. rules regarding data processing;
5. rules regarding processing of sensitive personal data;
6. rules regarding data subject rights;
7. rules regarding how public registers must treat personal data;
8. rules regarding data relating to criminal proceedings;
9. rules regarding making complaints to the Authority; and
10. rules regarding the transfer of personal data outside Bahrain.

DEFINITIONS

Definition of personal data

Personal data is defined under the PDPL as any information of any form related to an identifiable individual, or an individual who can be identified, directly or indirectly, particularly through their personal identification number, or one or more of their physical, physiological, intellectual, cultural or economic characteristics or social identity.

Definition of sensitive personal data

Sensitive personal data is a subset of personal data. It is personal data which reveals, directly or indirectly, the individual's race, ethnicity, political or philosophical views, religious beliefs, union affiliation, criminal record or any data related to their health or sexual life. Sensitive personal data requires more rigorous treatment by data controllers.

NATIONAL DATA PROTECTION AUTHORITY

Under the PDPL, the Authority will have power to investigate violations of the PDPL on its own, at the request of the responsible minister, or in response to a complaint.

The Authority can issue orders to stop violations, including issuing emergency orders and fines. Civil compensation is also allowed for any individual who has incurred damage arising from the processing of their personal data by the data controller, or violating

the provisions of the PDPL by a business's data protection officer. Finally, the most concerning feature of the PDPL for businesses is that it carries criminal penalties for violations of certain provisions.

Decree No. 78 of 2019 (the " **Decree**") was enacted to determine the administrative authority that will assume the mandated functions and powers of the Authority. This Decree came into force September 29, 2019.

Article I of the aforementioned Decree appoints the Ministry of Justice, Islamic Affairs and Endowments (the " **Ministry**") as the Authority for the protection of personal data in accordance with the provisions of the PDPL, on a temporary basis pending the financial allocation of the Authority in the general budget of Bahrain and the issuance of a decree forming the Board of Directors pursuant to Article 39 of the PDPL.

The Minister of the Ministry will assume the functions and powers prescribed to Board of Directors of the Authority and the Chairman of Board of Directors, in accordance with the provisions of the PDPL The Undersecretary of the Ministry will assume the same functions and powers as the Executive Chairman.

REGISTRATION

The Authority must create a register of data protection officers. To be accredited as a data protection officer, an individual must be registered in that register.

DATA PROTECTION OFFICERS

Data controllers may voluntarily appoint a data protection officer. The Authority's Board of Directors may also issue a decision requiring specific categories of data controllers to appoint data protection officers. However, in all instances, the data controller must notify the Authority of such an appointment within three days of its occurrence.

A data protection officer must help the data controller in exercising its rights and fulfilling its obligations prescribed under the PDPL The data protection officer also has a number of other roles, including liaising with the Authority, verifying that personal data is processed in accordance with the PDPL, notifying the Authority of any violations of the PDPL that the data protection supervisor becomes aware of and maintaining a register of processing operations that the data controller must notify the Authority about.

The Authority must create a register of data protection officers. To be accredited as a data protection officer, an individual must be registered in that register.

COLLECTION & PROCESSING

Processing is defined under the PDPL as any operation or set of operations carried out on personal data by automated or non-automated means, such as collecting, recording, organizing, classifying in groups, storing, modifying, amending, retrieving, using or revealing such data by broadcasting, publishing, transmitting, making them available to others, integrating, blocking, deleting or destroying them.

Processing of personal data can only occur with the consent of the data subject, unless the processing is necessary:

- to implement a contract to which the data subject is a party;
- to take steps at the request of the data subject to conclude a contract;
- to implement an obligation required by law, contrary to a contractual obligation or an order from a competent court;
- to protect the vital interests of the data subject; or
- to exercise the legitimate interests of the data controller or any third party to whom the data is disclosed, unless this conflicts with the fundamental rights and freedoms of the data subject.

Processing of sensitive personal data is also prohibited without the consent of the data subject, except when the processing:

- is required by the data controller to carry out their obligations;
- is necessary for the protection of the data subject;
- of the data is made available to the public by the data subject;

- is necessary to exercise any of the procedures of claims of legal rights or the defence thereof;
- is necessary for the purposes of preventive medicine, medical diagnosis, provision of healthcare, treatment or management of healthcare services;
- is carried out within the activities of associations, unions and other non-profit organisations;
- is carried out by a competent public entity; or
- is related to the race or ethnicity, if they are necessary to ascertain equal opportunities or treatment of the society's individuals.

Data controllers are prohibited from processing the following personal data types without the prior written authorization of the Authority:

- automatic processing of sensitive personal data of data subjects who cannot provide consent;
- automatic processing of biometric data;
- automatic processing of genetic data (unless such processing was provided by physicians and specialists at a licensed medical establishment and is necessary for purposes of preventative medicine or diagnostic medicine, or purposes to provide treatment or healthcare);
- automatic processing of personal data files that are in the possession of two or more data controllers that are processing personal data for different purposes; or
- processing that consists of visual recording to be used for monitoring purposes.

TRANSFER

Transfers of personal data out of Bahrain is prohibited unless the transfer is made to a country or region that provides sufficient protection to personal data. The Authority has listed the countries in which it deems provides adequate regulatory and legislative protection for personal data. Data controllers would be permitted to transfer personal data directly to the states, countries and territories listed in the regulation, without obtaining prior authorization from the Authority. The list of 83 countries are as follows:

- Andorra, Bulgaria, Denmark, French Guiana, Iceland, Argentina, Canada, Ecuador, Georgia, India, Australia, Chile, Egypt, Germany, Ireland, Austria, China, Estonia, Greece, Isle of Man, Belgium, Colombia, Falkland Islands, Guernsey, Israel, Bolivia, Croatia, Faroe Islands, Guyana, United Kingdom, Brazil, Cyprus, Finland, Hong Kong, Italy, Brunei, Czech Republic, France, Hungary, Japan, Luxembourg, Nigeria, Russia, Switzerland, Jersey, Macau, Norway, San Marino, Thailand, Jordan, Malaysia, Oman, Singapore, Ukraine, Kazakhstan, Malta, Pakistan, Slovakia, United Arab Emirates, Kingdom of Saudi Arabia, Mexico, Paraguay, Slovenia, United States of America, Kuwait, Monaco, Peru, South Korea, Uruguay, Latvia, Morocco, Poland, Spain, Vatican, Liechtenstein, Netherlands, Portugal, Suriname, Venezuela,Lithuania, New Zealand, Romania and Sweden.

Data controllers can also transfer personal data to countries that are not determined to have sufficient protection of personal data where:

- the transfer occurs pursuant to a permission to be issued by the Authority on a case-by-case basis, if it deems that the
- data will be sufficiently protected;
- if the data subject has consented to that transfer;
- if the data to be transferred has been extracted from a register that was created in accordance with the PDPL for the purpose of providing information to the public, regardless of whether viewing of this register is available to everyone or limited to the parties concerned in accordance with specific terms and conditions. In this instance, one shall have to satisfy the terms and conditions prescribed for viewing the register before viewing that information;
- if the transfer is necessary for any of the following:
    - to implement a contract between the data subject and the data controller, or to undertake preceding steps at the data subject's request for the purpose of concluding a contract;
    - to implement or conclude a contract between the data controller and a third party for the benefit of the data subject;
    - to protect the data subject's vital interests;

- to implement an obligation imposed by the PDPL (even if this is contrary to the contractual obligation), or to implement an order issued by a competent court, the public prosecution, the investigating judge or the military prosecution; or
- to prepare, execute or defend a legal claim.

SECURITY

The PDPL requires that data controllers apply technical and organizational measures capable of protecting the data against unintentional or unauthorized destruction, accidental loss, unauthorized alteration, disclosure or access, or any other form of processing.

The PDPL requires that the Authority's Board of Directors issues a decision specifying the terms and conditions that the technical and organizational measures must satisfy. The decision may require specific activities by applying special security requirements when processing personal data.

Data controllers must also use data processors who will provide sufficient guarantees about applying the technical and organizational measures that must be adhered to when processing the data. Data controllers must also take reasonable steps to verify that data processors comply with these measures.

BREACH NOTIFICATION

The data controller shall establish specific procedures to inform the Personal Data Protection Authority of the occurrence of any violation or breach of data within a period not exceeding (72) hours from the date of its discovery, unless if the such personal data breach would not affect the rights of data subjects.

ENFORCEMENT

The Authority can issue orders to stop violations, including emergency orders and fines. Civil compensation is also allowed for any individual who has incurred damage arising from the processing of their personal data by the data controller, or arising from the data protection officer's violation of the PDPL Appeals can be made against decisions of the Authority.

The PDPL also carries a range of criminal penalties and administrative fines for violating certain provisions.

Criminal penalties of imprisonment of not more than one year and / or a fine between BHD 1,000 to BHD 20,000, can be issued against any individual who:

- processes sensitive personal data in violation of the PDPL;
- transfers personal data outside Bahrain to a country or region in violation of the PDPL;
- processes personal data without notifying the Authority;
- fails to notify the Authority of any change made to the data of which they have notified the Authority;
- processes certain personal data without prior authorization from the Authority;
- submits to the Authority or the data subject false or misleading data to the contrary of what is established in the records, data or documents available at their disposal;
- withholds from the Authority any data, information, records or documents which they should provide to the Authority or enable it to review them in order to perform its missions specified under the PDPL;
- causes to hinder or suspend the work of the Authority's inspectors or any investigation which the Authority is going to make; and / or
- discloses any data or information which they are allowed to have access to, due to their job or which they used for their own benefit or for the benefit of others unreasonably and in violation of the provisions of the PDPL.

ELECTRONIC MARKETING

Under the PDPL, data controllers must notify the data subject when data is collected directly or indirectly of whether data will be used for direct marketing purposes. Notice is important because it alerts data subjects of their right to object to any direct marketing relating to their personal data.

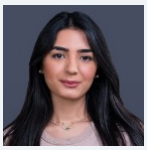
ONLINE PRIVACY

There is no specific online privacy regulation in Bahrain.

KEY CONTACTS

Mohamed Toorani
Legal Director - Head of Bahrain Office
T +973 1 755 0896
mohamed.toorani@dlapiper.com

Lulwa Alzain
Associate
T +973 1 755 0891
lulwa.alzain@dlapiper.com



Jenan Banahi
Associate
T +973 1755 0897
jenan.banahi@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BANGLADESH

Last modified 3 January 2024

LAW

Cyber al Security Act 2023 (**CA 2023**).

DEFINITIONS

Definition of personal data

Section 26 of the CA 2023 defines the term "identity information" as "*any external, biological or physical information or any other information which singly or jointly can identify a person or a system, such as name, photograph, address, date of birth, mother's name, father's name, signature, national identity card, birth and death registration number, finger print, passport number, bank account number, driving license, e-TIN number [Tax identification Number], electronic or digital signature, username, credit or debit card number, voice print, retina image, iris image, DNA profile, security related question or any other identification which are available for advance technology*".

Definition of sensitive personal data

The CA 2023 does not define the term "Sensitive Personal Data" or any similar or equivalent term.

NATIONAL DATA PROTECTION AUTHORITY

Cyber Security Agency.

REGISTRATION

No requirements.

DATA PROTECTION OFFICERS

No requirements.

COLLECTION & PROCESSING

There are no statutes that expressly allow the collection and processing of identification information.

The CA 2023 came into force in full on 18 September 2023 repealing the Digital Security Act 2018. The provisions of the CA 2023 closely mirror those of the Digital Security Act 2018, with the only modifications being a decrease in penalties for specific offenses. Section 26 of the CA 2023 has been drafted in very wide terms. The contents of this provision would appear to provide, *inter alia*, that if anyone **without lawful authority collects**, sells, keeps possession of, supplies or uses identification information of another person, it would constitute an offence[1]. The punishment for violation of Section 26 of the CA 2023 is imprisonment of a term not exceeding two years or a fine not exceeding Taka 5,00,000 (approx. US$ 4,545 as of 3 January 2023) or both.

Please note that the CA 2023 does not contain any exceptions to the Section 26 requirement. However, identification information may be, among other things, collected and stored by a person if he has **lawful authority**. The term "lawful authority" has not been defined in the CA 2023. The Government of Bangladesh has not yet issued any clarification as to what would constitute 'lawful use' and has provided no guidance on what would satisfy the 'lawful authority' requirement. It is for these reasons (among others) that the legislation has been widely criticised.

In our opinion, a person will be deemed to have lawful authority if they are authorized by statute or contract to collect and store such identification information.

1: Please note that this is an unofficial English translation of the wording of the provision in question.

TRANSFER

Bangladesh does not specifically regulate data transfers within Bangladesh or from Bangladesh to outside of Bangladesh. In our opinion, transfers would be permitted provided consent of the data subject is obtained.

While there are no general restrictions on transfer of data outside Bangladesh, please note that there are certain industry specific restrictions that are discussed below.

Banks

Section 12 of the Bank Companies Act, 1991 has imposed a restriction upon bank companies with regard to removal of documents and records outside Bangladesh without prior permission of Bangladesh Bank (i.e. the central bank of Bangladesh).

The requirement for obtaining prior written permission from Bangladesh Bank is upon the transferor, i.e. the bank company. Banks must also maintain confidentiality in banking transactions.

Telecommunication companies

The Bangladesh Telecommunication Regulatory Commission ("**Commission**") is the authority that is responsible for regulating telecommunications companies ("**telcos**") in Bangladesh and issuing licenses to telcos for providing mobile phone services.

The license which is granted to the telcos contains a provision regarding subscriber confidentiality. The confidentiality requirement applies to "*all information provided by the subscriber*". As such, telcos will be prohibited from sharing any subscriber information (to entities or persons located inside or outside Bangladesh) that does not come within the exemptions listed above. Furthermore, in our opinion, subscribers would not have the option of giving consent to the telcos to share their data, instead for such sharing, approval from the Commission will be required.

SECURITY

There are no data security requirements.

BREACH NOTIFICATION

There is no requirement to report data breaches to any individual or regulatory body.

ENFORCEMENT

There is no enforcement mechanism. Appropriate relief may be sought through courts of law having jurisdiction in the matter.

ELECTRONIC MARKETING

There is no regulation on electronic marketing.

ONLINE PRIVACY

There is no regulation on cookies and location data. However, it is advisable to obtain user consent, such as through appropriate disclaimers.

KEY CONTACTS

Dr. Kamal Hossain and Associates
www.khossain.com/

Dr. Sharif Bhuiyan
Partner and Deputy Head of Chambers – International and Commercial Practice
Dr. Kamal Hossain and Associates
T +88 02 9552946
sbhuiyan@khossain.com

Najeeb Huda
Senior Associate
Dr. Kamal Hossain and Associates
T +88 02 9552946
nhuda@khossain.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BARBADOS

Last modified 28 January 2024

LAW

The Data Protection Act (the "**Act**") was passed on August 12, 2019, and came into force in March 2021. The purpose of the Act is to regulate the collection keeping, processing, use and dissemination of personal data and to protect the privacy of individuals in relation to their personal data.

DEFINITIONS

Definition of Personal Data

"Personal data" means data which relates to an individual who can be identified:

- from that data; or
- from that data together with other information which is in the possession of or is likely to come into the possession of the data controller.

Definition of Sensitive Personal Data

"Sensitive personal data" means personal data consisting of information on a data subject's:

- racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- membership of a political body;
- membership of a trade union;
- genetic data;
- biometric data;
- sexual orientation or sexual life;
- financial record or position;
- criminal record; or
- proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court of competent jurisdiction in such proceedings.

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Commissioner (the "**Commissioner**") was appointed with effect from July 15, 2021 and is responsible for the general administration of the Act.

REGISTRATION

A data controller must be registered in the Register of Data Controllers.

A data processor must be registered in the Register of Data Processors.

DATA PROTECTION OFFICERS

The data controller and the data processor must designate a data privacy officer where:

- the processing is carried out by a public authority or body, except for a court of competent jurisdiction acting in their judicial capacity;
- the core activities of the data controller or the data processor consist of processing operations which, by virtue of their nature, their scope and their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the data controller or the data processor consist of processing on a large scale of sensitive personal data.

The data privacy officer must be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the duties and functions as set out under the Act.

COLLECTION & PROCESSING

Where personal data relating to a data subject is collected from the data subject, the data controller must, at the time when personal data is obtained, provide the data subject with the following:

- the identity and the contact details of the data controller and, where applicable, of the data controller's representative;
- the contact details of the data privacy officer, where applicable;

Processingof personal data is only lawful where:

- the data subject has given consent to the processing of his personal data for one or more specific purposes; or
- the processing is necessary
    - for the performance of a contract to which the data subject is a party;
    - for the taking of steps at the request of the data subject with a view to entering into a contract;
    - for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract;
    - in order to protect the vital interests of the data subject;
    - for the administration of justice;
    - for the exercise of any functions of either House of Parliament;
    - for the exercise of any functions conferred on any person by or under any enactment;
    - for the exercise of any functions of a public authority;
    - for the purposes of legitimate interests pursued by the data controller or by the third party to whom the data is disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject; or
    - processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

TRANSFER

Transfer of personal data is unlawful unless certain conditions are satisfied. Where the data subject has given their consent to the transfer of their personal data, the restrictions on the transfer of the data do not apply. The Act also sets out various other exemptions for the restrictions where transfer of the personal data is necessary e.g. for the performance of a contract between the data subject and the data controller, reasons of substantial public interest, for the purpose of obtaining legal advice, etc.

Personal data obtained must not be transferred to a country or territory outside Barbados unless that country or territory provides for (a) an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of

personal data and (b) appropriate safeguards on condition that the rights of the data subject are enforceable and there are available, effective legal remedies for data subjects.

The circumstances for determining an adequate level of protection as well as methods for providing appropriate safeguards including the development of binding corporate rules must submitted to the Commissioner for authorisation.

The "*binding corporate rules*" must specify (but not limited to) the following:

- the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
- the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
- their legally binding nature, both in and outside of Barbados.

SECURITY

The data controller and the data processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

BREACH NOTIFICATION

In certain circumstances, a data controller is required to report to the Commissioner data breaches which have affected a data subject.

Mandatory breach notification

Where there is a personal data breach the data controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of an individual.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the data controller must communicate the personal data breach to the data subject without undue delay and, where feasible, not later than 72 hours after having become aware of it.

ENFORCEMENT

Where the Commissioner is satisfied that a data controller or a data processor has contravened or is contravening this Act, the Commissioner may serve him an "enforcement notice".

In deciding whether to serve an enforcement notice, the Commissioner must consider whether the contravention has caused or is likely to cause any person damage or distress.

ELECTRONIC MARKETING

There are no specific laws in respect of these matters.

ONLINE PRIVACY

There are no specific laws in respect of these matters.

KEY CONTACTS

Chancery Chambers
chancerychambers.com/

Angela R Robinson

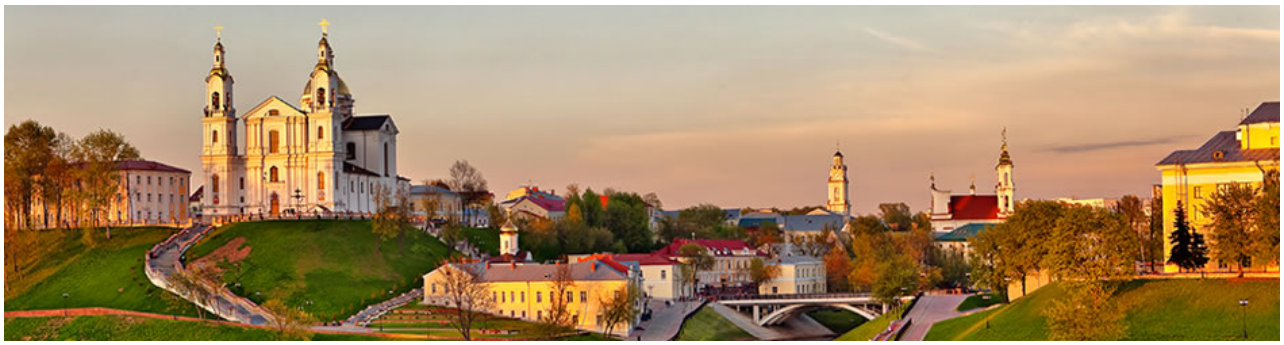
Senior Associate
Chancery Chambers
T +246 431 0070
arobinson@chancerychambers.com

Giles A M Carmichael
Partner
Chancery Chambers
T +246 431 0070
gcarmichael@chancerychambers.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BELARUS



Last modified 17 January 2024

LAW

The fundamental legal act regulating personal data protection in Belarus is the Law on Personal Data Protection of 7 May 2021 No. 99-Z which entered into force on 15 November 2021 (Data Protection Law). It is the first Belarusian legal act intended specifically for regulation of personal data protection issues.

It worth also to take into consideration the acts implemented within the framework of the Eurasian Economic Union (EEU), e.g. the Protocol on Information and Communication Technologies and Informational Interaction within the Eurasian Economic Union, Annex 3 to the Treaty on the Eurasian Economic Union of 29 May 2014. Following the Decision of the Supreme Eurasian Economic Council of 11 October 2017 the member states of EEU are planning to develop the initiative on conclusion of the Agreement on Data Circulation within the Union (including on personal data protection). The initiative is one of measures aimed at implementation of the Main Directions for Implementation of the Digital Agenda of the Eurasian Economic Union until 2025.

DEFINITIONS

Definition of personal data

Data Protection Law defines “personal data” as any information relating to an identified or identifiable natural person.

In its turn, “individual who can be identified” means an individual who can be directly or indirectly determined, in particular through the surname, proper name, patronymic, date of birth, identification number, or through one or more of characteristic features of her / his physical, psychological, mental, economic, cultural or social identity.

The Law also defines “special personal data”, “biometric personal data”, “genetic personal data” and “publicly available personal data”.

Definition of sensitive personal data

Data Protection Law defines “special personal data” which include information about race, nationality, political, religious and other convictions, health and sexual activity; criminal conviction records; biometric and genetic personal data.

“Biometric personal data” means information describing the physiological and biological characteristics of a person, which is used for her / his unique identification (fingerprints, palms, iris, characteristics of the face and its image, etc.), while “genetic personal data” is defined as information related to the inherited or acquired genetic characteristics of a

person, which contain unique data on her / his physiology or health and can be identified, in particular, during the study of her / his biological sample.

NATIONAL DATA PROTECTION AUTHORITY

The National Personal Data Protection Centre ("**NPDPC**") is the competent authority for the protection of personal data subjects' rights. The main tasks of the NPDPC are taking measures to protect the rights of personal data subjects in the processing of their personal data and organising training on personal data protection issues.

In accordance with these tasks NPDPC performs the following functions:

- controls the processing of personal data by operators (authorised persons);
- considers complaints of personal data subjects regarding the processing of personal data;
- determines the list of foreign countries having proper level of data subjects’ rights protection;
- issues permits for cross-border transfer of personal data, if the level of protection of personal data subjects' rights in a foreign country is not adequate, as well as establishes the procedure for issuing such permits;
- makes proposals on the improvement of the personal data legislation, participates in the drafting of legal acts on personal data;
- provides explanations on the application of personal data legislation, carries out other explanatory work on personal data legislation;
- determines the cases in which it is not necessary to notify NPDPC of the breach of personal data protection systems;
- establishes the classification of information resources (systems) containing personal data in order to determine the technical and cryptographic protection requirements for personal data;
- participates in the work of international organisations on personal data protection issues;
- cooperates with authorities (organisations) for protection of rights of personal data subjects in foreign countries;
- publishes annually by 15 March, the report in mass media on its activities;
- implements educational programs of additional education for adults in accordance with the legislation on education;
- exercises other authority established by the personal data legislation.

NPDPC constantly develops legislation in a field of personal data protection. Data protection authority publishes its recommendations and clarifications on application of Data Protection Law provisions and specifics of personal data protection on various matters (*inter alia*, on the content of privacy policy, on personal data processing in employment and pre-employment relations, in educational sphere, on relations between operators and authorised persons in terms of personal data processing).

Contact information of NPDPC

Build. 24-3
K.Zetkin str.
Minsk, 220036

T: + 375 17 367 07 90

e-mail: info@cpd.by

REGISTRATION

Since 1 January 2024 operators are obliged to add information about information resources (systems) containing personal data into Register of Personal Data Operators and ensure that the relevant information is kept up-to-date. Information shall be added regarding information resources (systems) that involve:

- cross–border transfer of special personal data, to a foreign state with “inappropriate” level of data subjects’ rights protection (special except for certain cases provided by Data Protection Law);
- processing of biometric and (or) genetic personal data;
- personal data processing of more than 100 thousand individuals; and
- personal data processing of more than 10 thousand individuals under the age of sixteen.

Order of the Operational and Analytical Centre under the President of the Republic of Belarus (OAC) No. 94 of 1 June 2022 establishes the list of data that shall be added into the Register of Personal Data Operators.

State information systems shall be registered under the separate procedure regardless whether any personal data are processed in it or not. According to Belarusian legislation state information systems are information systems created and / or acquired at the expense of state or local budgets, state off-budget funds, or by state legal entities. Registration is performed by specially authorised by the Ministry organisation – SERUE “Institute of Application Software Systems”. One of the conditions for state registration of an information system is registration of all information resources included in such an information system. Described registration can be performed for private owned information systems voluntarily.

According to the Edict of the President of the Republic of Belarus of 16 April 2013 No. 196 On Certain Measures for Improvement of the Information (Information Protection Edict) organisations owning information systems intended for processing of personal data are obliged to notify the OAC on the conditions of technical information protection of such systems.

DATA PROTECTION OFFICERS

Data Protection Law obliges operators to designate a structural unit or person responsible for the internal control of personal data processing. This shall be an internal unit or employees of the organisation, i.e. it is not possible to outsource the control functions. The legislation establishing obligations of different positions stipulates that the specialist of internal control over personal data processing shall have higher education, while no requirements for work experience are established.

Persons responsible for the internal control of personal data processing shall complete training on issues related to personal data protection at least once every five years. Depending on the type of organisation, the training may be organised at NPDPC or other educational organisations. In addition, the operators shall annually by 15 November provide NPDPC with information on the number of persons who shall complete training at NPDPC.

Moreover, a legal entity, including state body, processing personal data shall create information protection systems to secure information in their information systems used for processing of such data. As a part of creation of such system the entity should establish special department or appoint employee responsible to take required technical and cryptography information protection measures. According to the Information Protection Edict, the employees of such department (responsible employee) are required to have higher education in the sphere of information protection security or other higher or specialised secondary or professional - technical education and undergo training on the issues of technical and cryptographic information protection.

If for some reasons respective departments / employees cannot take such measures themselves, a special organisation licensed to perform activities on technical and / or cryptography information protection may be involved.

COLLECTION & PROCESSING

Data Protection Law contains a wide range of legal bases for personal data processing:

- data subject’s consent;
- if the processing is required for:
    - administrative or criminal proceedings, operational-search activities;
    - administration of justice and the enforcement of court orders and other enforcement documents;
    - performing monitoring activities (supervision) in accordance with the legislation;

  - implementation of legislation on national security, on combating corruption, on preventing money laundering, financing of terrorist activities and financing weapons of mass destruction proliferation;
  - the implementation of legislation on elections and referendum;
  - state social insurance purposes;
  - formalising employment relationships, in the process of employment activities;
  - notarial activities;
  - Belarusian citizenship issues;
  - assignment and payment of pensions, benefits;
  - the organisation and carrying out of national statistical observations;
  - scientific and other research purposes, on condition that the personal data are depersonalised;
  - accounting, calculation, charging of fees for housing and utility services, other services, taxes;
- processing is based on a contract, that is concluded (being concluded) with data subject, and for the purpose of performing actions stipulated by this contract;
- if personal data are specified in a document addressed to the operator and signed by the data subject;
- processing is essential for the performance of certain journalist’s activities;
- processing is required to protect the subject's life, health or other interests if obtaining of consent is not possible;
- if personal data were previously disseminated;
- in order to fulfil the duties / powers stipulated in legislation;
- in other cases expressly provided in legislation.

Data Protection Law has different list of legal bases for processing of special personal data and for cross-border transfer of personal data to the territories of states that do not ensure proper protection of data subjects rights.

The consent of the data subject can be obtained in writing, in the form of an electronic document or in another electronic form (e.g. via tick-box at the website or SMS / email verification). Operator shall provide proof, if be required, that it has collected proper consent for personal data processing.

Before obtaining consent, the operator shall provide the subject of personal data with the following information:

- name (full name) and location (address of residence) of the operator;
- purpose of personal data processing;
- list of personal data to be processed;
- consent validity term;
- information about the persons authorised by operator to process personal data (if those are engaged);
- what actions be done with personal data;
- a general description of the processing methods;
- other relevant information.

In addition, apart from other necessary information, the subject shall be informed of his/her rights, the mechanism for exercising them, the consequences of giving and withdrawing consent.

Operator may collect surname, first name, middle name of data subject, date of birth, identification number (if not, the number of the ID document) only if it is required for the purposes of processing. Such information shall be provided by data subject when at the time he/she provides the consent.

Collection and processing of personal data shall be performed having implemented certain legal, organisational and technical measures for personal data protection. The organisational measures may include establishing a special entrance regime to the premises used for collection and processing, designation of employees who can have an access to such premises and data, and differentiation of access levels to respective information. The technical measures may include using cryptography, technical means and other possible measures of control over information protection.

TRANSFER

The general rule is that cross-border transfer is prohibited, unless a foreign state provides an appropriate level of protection of the personal data subjects’ rights. NPDPC has established that the list of foreign states, which ensure appropriate level of protection. The list includes foreign states that are parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted in Strasbourg on 28 January 1981 as well as foreign states that are members of the Eurasian Economic Union. There are certain plans to broaden the list of foreign states that provide appropriate level of protection of the personal data subjects’ rights.

However there are certain exceptions, when transfer to the jurisdictions with inappropriate level of protection will be allowed. For example, upon respective consent of the personal data subject and informing of the possible risks or under the individual permit for cross-border transfer issued by NPDPC.

SECURITY

The owners of the information systems should take appropriate technical, legal and organisational measures to secure personal data processed in their information systems. The key technical measure is creation of the information protection system to secure the information system of an entity intended for processing of personal data. The information protection system shall be attested according to the procedure established by the OAC. The rules also suggest simplified attestation procedure for subjects using information system of other organisations who have already passed attestation procedure for their systems.

BREACH NOTIFICATION

Data Protection Law establishes an obligation to notify NPDPC on breach of systems used for personal data protection immediately, but not later than within three business days of discovery, in writing or in the form of an electronic document. Exceptions to this requirement are cases where a breach of security systems has not resulted in the unlawful dissemination, provision of personal data; modification, blocking or deletion of personal data without the possibility of restoring access to it.

Certain additional requirements on the notification of the OAC are set for specific cases of information protection system breaches or periodical reporting as required by Belarus law. The respective requirements are set forth in the Regulations on the procedure for submitting information about information security events, the state of technical and cryptographic protection of information to the OAC, as approved by the Order of the OAC of 2 February 2020 No. 66.

ENFORCEMENT

According to Data Protection Law, NPDPC supervises the processing of personal data by operators and authorised persons. In the case of a breach of personal data legislation, NPDPC has the right to issue a demand to eliminate the detected violations and / or to terminate personal data processing in the information resource (system). Term for elimination and / or termination is set by the NPDPC, but shall not be longer than six months.

Violation of personal data protection legislation may result in civil, criminal and administrative liability. If the violation has led to moral damages, the violator may be required by the court to reimburse such damages.

Administrative Offences Code of Republic of Belarus stipulates specific sanctions for personal data processing violations, including:

- intentional illegal collection, processing, storage or transfer of personal data of an individual or violation of his / her rights related to the processing of personal data may cause a fine up to 50 base units; intentional distribution – up to 200 base units (since 1 January 2023 one base unit equals BYN 37, approx. EUR 11);
- **non-compliance with requirements on data protection** measures implementation may cause a fine ranging from 20 to 50 base units for legal entities.

The Criminal Code of Republic of Belarus envisages criminal liability for the following breaches:

- unlawful collection or provision of information relating to the private life and (or) personal data of another person without his / her consent (depending on the circumstances like volume on gravity) causing substantial harm to the rights,

freedoms and legitimate interests of a citizen a person could be sentenced to community work, a criminal fine, arrest, or the restriction or deprivation of liberty for up to two years. For the unlawful distribution – restriction or deprivation of liberty for up to three years with the criminal fine. Higher liability may apply if offence relates to the victims performing public functions; failure to comply with measures to ensure the protection of personal data by a person who processes personal data, which has inadvertently resulted in their dissemination and causing serious consequences a person could be sentenced to a criminal fine, deprivation of the right to occupy certain job positions or perform certain activities, corrective work for up to one year, arrest, or the restriction of liberty for up to two years or deprivation of liberty for up to one year.

ELECTRONIC MARKETING

Electronic marketing is subject to the rules established by the Law on Advertising of 10 May 2007 No. 225-Z (Advertising Law) and the Law on Mass Media of 17 July 2008 No. 427-Z (Mass Media Law).

According to the general rule of the Advertising Law it is not allowed to use in advertising names, pseudonyms, images or statements of citizens of the Republic of Belarus without their consent or the consent of their legal representatives.

Distribution of advertisements by telecommunication means (e.g. telephone, telex, facsimile, mobile telephone communications, email) can be performed only with the consent of respective subscriber or addressee. Such consent can be made as a text document, including document in electronic form. The consent also can be a part of an agreement for telecom services. In this case subscriber or addressee must be informed about her / his right to demand stopping placing (distributing) advertisement to her / him, which shall be specifically confirmed by the subscriber (addressee).

The advertisement distributor is obliged to immediately stop advertising to subscriber or addressee upon his / her demand within one work day from receiving the demand.

Individuals whose rights have been violated as a result of creation and / or distribution of an advertisement are entitled to protect their rights in court proceedings.

According to the Mass Media Law, information about person’s personal life or audio, video records and photos of a person can be distributed in mass media as a general rule only with consent of such person or his/her authorised representative. As an exception, distribution in the media of information messages and (or) materials prepared using audio or video recording, filming or photo of an individual without her / his consent is allowed only if measures are taken against the possible identification of this individual by unauthorized persons, and also provided that the dissemination of these information messages or materials does not violate the constitutional rights and freedoms of the individual and is necessary to protect public interests (except to criminal investigations or court proceedings).

ONLINE PRIVACY

Belarus law does not specifically regulate online privacy. General requirements on personal data protection apply.

Certain specific online privacy requirements can be established under the legislation. For example, personal data of a person, who is a domain name administrator, can be disclosed in online WHOIS service of Belarusian domain zone only with consent of such person. However, consent is not required if the domain name was registered in the name of an individual entrepreneur.

KEY CONTACTS

Sorainen
www.sorainen.com/

Kirill Laptev
Partner
Sorainen
T +375 17 391 2061
kirill.laptev@sorainen.com

Veranika Amelyanchuk
Associate
Sorainen
T +375 17 391 2061
veranika.amelyanchuk@sorainen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BELGIUM

Last modified 6 February 2024

LAW

The GDPR has been integrated in Belgium through a few laws. The 'Data Protection Act' of July 30, 2018 provides for the implementation of some of the GDPR provisions open to further definition, derogation or additional requirements. It also includes the transposition of the 2016/680 Directive regarding the processing of personal data in the criminal justice chain and the establishment of a Control body on police information (called 'COC'). Additionally, it regulates the authorities outside the scope of the EU law (including intelligence and security services).[1]

The Belgian Data Protection Authority, the successor of the Belgian Privacy Commission, was established by the Belgian Federal Chamber of Representatives by the Act of December 3, 2017 ("**DPA Act**")[2]. Several other laws have also been adapted to align them with the GDPR (e.g. Video Surveillance Act).

The competent Secretary of State has announced legislative proposals for a reform of Belgian data protection law (i.e. both the Data Protection Act and DPA Act). The reform proposal of the Data Protection Act has been introduced before the Federal parliament and currently sits at the level of inter-cabinet operations. If approved, it will go to the Council of Ministers and subsequently to the COC and Council of State for advice. Delays are possible as stakeholders might view it as an ideal opportunity to address specific longstanding issues. The exact timing of adoption is thus currently unclear. The reform proposal of the DPA Act has been approved by the Chamber of Representatives on 14 December 2023. The reform of the DPA Act intends to strengthen the functioning, the independence and the pragmatic approach and sectoral expertise of the Belgian Data Protection Authority.

In addition to the above-mentioned reform of the DPA Act, there has been another legislative proposal to amend this Act due to a judgment of the Belgian Constitutional Court. The Court found Article 108 of the DPA Act to be unconstitutional insofar it does not allow interested third parties to appeal a decision of the Litigation Chamber. To accommodate the Court’s findings the proposal provides in the opportunity for third parties to appeal decisions of the Litigation Chamber before the Market Court and to intervene in the proceedings before the Litigation Chamber.

---

1. See Data Protection Act.
2. See DPA Act.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor " *processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Data Protection Act builds on the definitions contained in the GDPR and further clarifies some notions, such as the notion of 'public authority'[1]. It further adds the definitions of a ‘**trusted third party**’, ‘ **disclosure of personal data’** and ‘**distribution of personal data**’ in the context of the research and statistical purposes exception. The Data Protection Act also clarifies certain concepts such as 'processing in the substantial public interest'[2], the 'processing for journalistic purposes'[3] and introduces new concepts such as 'a joint database'[4].

1. Art. 5 Data Protection Act.
2. Article 8 para. 1 Data Protection Act.
3. Art. 24 para. 1 Data Protection Act.
4. Article 48 Data Protection Act.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The DPA Act establishes the Data Protection Authority as the successor of the Privacy Commission which was established under the old data protection legislation. The Data Protection Authority has the competences as set out in the GDPR whenever that competence has not been explicitly assigned to another body.

The Data Protection Act appoints three more regulatory authorities at the federal level (COC[1], Committee I[2] and Committee P[3]) with varying data protection related competences next to the general Data Protection Authority. In addition, there are also regional supervisory authorities who have been entrusted mainly with the supervision of the public authorities of the regions.

The composition of the Data Protection Authority has proven controversial due to the involvement of some members in government bodies. The European Commission warned Belgium mid 2021 that it would start an infringement procedure before the EU Court of Justice if the problems regarding the Data Protection Authority’s independence would not be resolved. Therefore, a legislative proposal has been introduced before the Federal Parliament at the end of 2021 to amend the DPA Act by partially reforming the rules on the composition of the Data Protection Authority[4]. Additionally, a revocation procedure was initiated by the Belgian federal parliament in March 2022 following an audit of the Belgian Court of Auditors. The Belgian Chamber of Representatives voted to revoke the mandate of two directors of the Data Protection Authority under the so-called Article 45 procedure of the DPA Act. As the Chamber’s decision is not public, the exact allegations and reasons for revocation of the mandates are unknown. In 2023, the two mandates have been reinstated. Two new directors have been appointed at the Data Protection Authority. Hopefully, this will bring about more stability as it is clear that these events were testing / challenging the well-functioning of the Data Protection Authority.

1. Art. 231 Data Protection Act.
2. Art. 72 para. 2 °7 Data Protection Act.
3. Art. 26 °7, c) Data Protection Act.
4. Legislative proposal 26 November 2021, amending the Act of 3 December 2017 establishing the of the Data Protection Authority, in order to modify the composition of the centre of expertise so that the independence of its members its members can be guaranteed (Doc. No. 55-2347/001), www.lachambre.be/flwb/pdf/55/2347/55K2347001.pdf

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

The registration of processing activities through a notification has been abolished. However, in the public sector, the Data Protection Act obliges the controller of processing activities in the context of police services to publish a protocol detailing the transfer to a public authority or private body based on public interest and compliance with legal obligations[1].

1. Art. 20 Data Protection Act.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

In addition to the GDPR, the Data Protection Act requires the appointment of a DPO depending on the impact of the processing activity, namely if it may entail a high risk as referred to in article 35 of the GDPR when (i) a private law body processes personal data on behalf of a federal public authority or a federal public authority transfers personal data to this private law body in the context of police services[1] or (ii) the processing falls under the exception necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes[2]. Some public authorities regulated by the Data Protection Act are also required to appoint a DPO[3].

The Data Protection Authority has addressed the GDPR requirements for the appointment of DPOs and the exercise of its tasks in several cases, including in relation to the position of the DPO and its independence, the obligation to directly report to the highest management level, the necessary resources to carry out his tasks and the requirement that a DPO must have “expert knowledge”.

1. Art. 21 Data Protection Act.
2. Art. 190 Data Protection Act.

3. The Center for Missing and Sexually Exploited Children (Child Focus) Art. 8 para. 3 Data Protection Act; Competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security implementing Directive 2016 /680 Art. 63 et seq Data Protection Act; Intelligence and security services Art. 91 Data Protection Act; Bodies for security clearances, certificates and recommendations Art. 124 Data Protection Act; Coordination Unit for Threat Assessment Art. 157 Data Protection Act.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or

have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Data Protection Act adds only specificities to the general processing requirements. The age for consent of children for the purposes of article 8.1 GDPR is 13 year[1]. When processing genetic, biometric and health data, a controller needs to indicate who has access to these personal data, keep a list of the categories of people who have access to these data, keep this list at the disposal of the DPA, and ensure that these people are bound by a legal, statutory or contractual obligation of confidentiality[2]. The Data Protection Authority has adopted specific guidelines regarding the processing of biometric data[3].

The Data Protection Act also provides a list of legal bases for processing data relating to criminal convictions and offences and requires an access management list and confidentiality duties (as described here above) for processing such data[4].

Data subject rights

The Data Protection Act provides further exceptions to data subject’s rights, including the right to be informed when personal data is received from authorities under special regimes[5] or when personal data is disclosed to these bodies [6]. With respect to the special regimes addressed in the Data Protection Act, the Data Protection Act also sets out the corresponding data subject rights (which are often more limited than those included in the GDPR)[7].

The Data Protection Act clarifies that data subject rights, including the right to information in judicial proceedings /decisions, will be accommodated in accordance with the Judicial Code, the Code on Criminal proceedings and any specific laws related to criminal law procedure[8].

1. Art. 7 Data Protection Act.
2. Art. 9 Data Protection Act.
3. Data Protection Authority, Recommendation on the processing of biometric data (No. 1-2021, 1 December 2021).
4. Art. 10 Data Protection Act.
5. Art. 11, Art. 13 and Art. 14 Data Protection Act.

6. Art. 12 Data Protection Act.
7. Art. 36 et seq, Art. 79, Art. 105 (9), Art. 113, Art. 145, Art. 173 Data Protection Act.
8. Art.16 Data Protection Act.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU - U.S. Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

No general additional requirements relating to transfers are introduced by the Data Protection Act. The Data Protection Act only regulates the transfer of personal data under the special regimes, which in certain cases provides for less leeway for transfers[1].

For more information, please visit our Transfer - global data transfer methodology website.

1. Art. 66-70, Art. 93-94, Art. 126-127, Art. 159-160 Data Protection Act.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The Data Protection Act inserts no general additional requirements in relation to security measures. In the context of archiving, scientific or historical research purposes or statistical purposes, the Data Protection Act sets out specific rules including anonymization or pseudonymization requirements[1].

Security measures are also detailed for each special regime but resemble the GDPR[2].

---

1. Art. 198 et seq Data Protection Act.
2. Intelligence and security services Art. 88-89 Data Protection Act, Bodies for security clearances, certificates and recommendations Art. 121-122 Data Protection Act, Coordination Unit for Threat Assessment Art. 154-155 Data Protection Act, Passenger Information Unit Art. 179-180 Data Protection Act.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

No general additional requirements are inserted in the Data Protection Act relating to data breaches.

Data breach obligations are also detailed for each special regime, but they resemble those contained in the GDPR.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

In addition to the GDPR, the Data Protection Act introduces a specific procedure for actions for injunctions that can be initiated by the data subject or by the Data Protection Authority (DPA)[1]. These claims should be brought before the President of the Court of First Instance except when the personal data is processed in criminal investigations or procedures[2]. There is no single court territorially competent to hear these claims[3].

The Data Protection Act also contains a legal basis that allows a body, organisation or non-profit organisation to represent the data subject upon its request when it:

- was founded in accordance with Belgian law
- has legal personality
- has statutory objectives of public interest
- has been active in the area of the protection of personal data for at least 3 years[4]

The DPA can impose administrative fines under article 83 of the GDPR[5], but public authorities, their agents and authorised representatives are exempted insofar they are not offering goods or services on the market[6]. A supervisory authority can exercise the corrective measures set out in article 58.2 GDPR but with regard public authorities, only over the categories enumerated in the Data Protection Act[7].

Depending on the infringement and the infringer, the controller, processor, competent public authority or their agent can be subjected to criminal sanctions, such as criminal fines between 800 EUR – 160.000 EUR and a publication of the judgement[8].

The DPA consists of 6 different Committees. The **Inspection Committee** of the DPA enjoys investigation powers, such as to identify persons, interview persons, conduct written interrogations, conduct on-site investigations, consult information systems and copy the data they contain, consult information electronically, seize or seal goods or computer systems and demand the identification of the subscriber or the normal user of an electronic communication service or of the electronic means of communication used[9]. Additionally, the inspector-general and the inspectors of the inspection committee may order the temporary suspension, restriction or freezing of the data processing activities that are the subject of an investigation if this is necessary to avoid a serious, immediate and difficult to repair disadvantage.[10] They can also request further information[11].

The **Litigation Chamber** can *inter alia* follow-up on a complaint but also propose a settlement, formulate warnings and reprimands, order compliance with data subjects’ requests to exercise their rights, order the suspension of cross-border data flows and can also impose periodic penalty payments and/or administrative fines[12].

Specific provisions according to Art. 85 to 87 and Art. 89 GDPR

The legislator has made use of the opportunity offered by the GDPR to provide exemptions or derogations from certain obligations when the processing is carried out for journalistic purposes and the purposes of academic, artistic or literary expression. For those purposes, the Data Protection Act exempts the controller not only from respecting certain data subjects’ rights under the GDPR but also some obligations of the controller (e.g. notification in case of breaches, transfer requirements, etc) and the investigative powers of the DPA[13].

The Data Protection Act also introduces two regimes for the derogations relating to the processing for archiving, scientific or historical research purposes or statistical purposes:

- general safeguards requiring among others register, information[14], contractual[15] and security requirements, or
- compliance with a code of conduct[16]

The Data Protection Act does not include other derogations relating to employment.

---

1. Art. 211 par. 3 Data Protection Act.
2. Art. 209 Data Protection Act.
3. Art. 209 par. 2 Data Protection Act.
4. Art. 220 par. 2 Data Protection Act.
5. Art. 101 DPA Act
6. Art. 221 par. 2 Data Protection Act.
7. Art. 221 par. 1 Data Protection Act.
8. Art. 222 et seq Data Protection Act.
9. Art. 66 DPA Act.
10. Art. 70 DPA Act.
11. Art. 76 DPA Act.
12. Art. 95 DPA.
13. Art. 24 Data Protection Act.
14. Art. 193 Data Protection Act.
15. Art. 194 Data Protection Act.
16. Art. 187 Data Protection Act.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Data Protection Act applies to most electronic marketing activities, as there is likely to be processing of personal data involved (e.g. an email address is likely to be ‘personal data’ for the purposes of the Data Protection Act). The Data Protection Act does not contain additional rules to the GDPR for the use of personal data for the purposes of electronic marketing.

However, specific rules are set out in the Belgian e-commerce legislation (Book XII of the Code of Economic Law) regarding opt-in requirements:

- These rules apply to all ‘electronic messages’, such as emails and text messages (Short Message Systems or SMS). Other types of electronic communication such as instant messaging and chat may also fall within the scope of these rules depending on the specific context. This covers not only clear promotional messages, but also newsletters and similar communications. Indeed, any form of communication intended to directly or indirectly promote goods, services, the image of a company, organisation or person which/who exercises a commercial, industrial or workmanship activity or regulated profession falls within the scope of these rules.

- As a general principle, the prior, free, specific and informed consent of the recipient of the message must be obtained (‘opt-in principle’).

- Two exceptions apply to the opt-in principle. No prior, free, specific and informed consent is to be obtained if:

  - the electronic marketing message is sent to existing customers of the service provider, or

  - the electronic message is sent to legal persons (e.g. to a general email address such as info@company.com).

  These exceptions are subject to compliance with strict conditions.

- Furthermore, all electronic messages must contain a clear reference to the recipient's right to opt out, including means to exercise this right electronically.

Neither the Data protection Act nor the DPA Act include specific provisions on electronic marketing.

The Data Protection Authority has adopted specific guidelines regarding direct marketing[1].

---

1. Data Protection Authority, Recommendation on the processing of personal data for direct marketing purposes (No. 1-2020, 17 January 2020).

ONLINE PRIVACY

Cookies

Article 5 (3) of the E-Privacy Directive was initially implemented into Belgian Law by means of an amendment to article 129 of the Belgian Electronic Communication Act. By the Act of 21 December 2021 transposing the European Electronic Communications Code and amending various provisions on electronic communications, article 129 was abolished and a similar provision was inserted in the Belgian Data Protection Act by means of a new article 10/2. This amendment explicitly confirms the competence of the Belgian Data Protection Authority regarding cookies.

The use and storage of cookies and similar technologies requires:

- the provision of clear and comprehensive information; and
- consent of the website user.

Consent is not required for cookies that are:

- used for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or
- strictly necessary for the provision of a service requested by the user.

The DPA has provided useful additional guidance related to topics such as cookie walls, social media plugins and the validity of consent through browser settings. Recently it published a so called ‘Cookie Checklist’ as a guidance tool for

companies to ensure the compliant use of cookies. Furthermore the DPA has taken several enforcement decisions with regard to cookies.[1]

Download DLA Piper's Guide on Cookies.

Location data

As location data are personal data, the processing of these data must comply with the general rules stipulated by the GDPR and the Data Protection Act (including, depending on the context, article 10/2). Neither the Data Protection Act nor the DPA Act include any other specific provisions on location data.

In addition, article 123 of the Belgian Electronic Communication Act stipulates that mobile network operators may process location data of a subscriber or an end user only to the extent that the location data has been anonymised, or if the processing is carried out in the framework of the provision of a service regarding traffic or location data.

The processing of location data in the framework of a service regarding traffic or location data is subject to strict conditions set forth in article 123.

Traffic data

As traffic data constitute personal data, the processing of traffic data must comply with the general rules stipulated by the GDPR and the Data Protection Act (including, depending on the context, article 10/2) . Neither the Data Protection Act nor the DPA Act include any other specific provisions on traffic data.

However, in accordance with article 122 of the Belgian Electronic Communication Act, mobile network operators are required to delete or anonymise traffic data of their users and subscribers as soon as such data is no longer necessary for the transmission of the communication (subject to compliance with cooperation obligations with certain authorities).

Subject to compliance with specific information obligations and subject to specific restrictions, operators may process certain traffic data for the purposes of:

- invoicing and interconnection payments;
- marketing of the operator’s own electronic communication services or services with traffic or location data (subject to the subscriber’s or end user’s prior consent); and
- fraud detection.

1: I.a. Decision on the merits, 21 January 2022, nr. 11/2022; Decision on the merits, 24 May 2022, nr. 84/2022; Decision on the merits, 25 May 2022, nr. 85/2022; Decision on the merits, 16 June 2022, nr. 103/2022.

KEY CONTACTS

Kristof De Vulder
Partner
T +32 (0) 2 500 15 20
kristof.devulder@dlapiper.com

Heidi Waem
Counsel
T +32 2500 1614
heidi.waem@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BENIN

Last modified 8 January 2024

LAW

The data protection regime in Benin is governed by two pieces of legislations namely the Law No. 2017-20 of April 20, 2018 on the digital code and the Law No. 2009-09 of May 22, 2009 Dealing with the Protection of Personally Identifiable Information.

The Law on the digital code deals with the collection, treatment, transmission, storage, and use of personal data by a person, the state, local authorities, and legal persons, as well as automated processing and non-automated processing of personal data contained in files, or any processing of data for public security, defense, research, prosecution of criminal offenses, or the security and essential interests of the state.

By contrast, the Law on the Protection of Personally Identifiable Information relates to the digital processing of personally identifiable information in digital files or manuals, as well as personal identification mechanisms based on nominative, personal, and biometric information processed alongside a national ID number.

DEFINITIONS

Definition of Personal Data

The personal data is defined as any information relating to an identified or identifiable natural person. It makes a direct reference to sound and image (Article 1 of the Digital Code).

Definition of Sensitive Personal Data

Pursuant to Article 1 of the Digital Code, the following personal data is considered 'sensitive' and is subject to specific processing conditions: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade union membership; genetic data; and health-related data; data concerning a person's sex life or sexual orientation, prosecution to criminal and administrative penalties.

NATIONAL DATA PROTECTION AUTHORITY

The APDP (The Beninese data protection authority) is the regulator for data in the Republic of Benin. It is an independent and administrative body with a legal personality as it ensures the application of the provisions of the Digital Code and the right to privacy.

The APDP’s powers and responsibilities which include:

- raising public awareness of the risks, rules, and rights surrounding the processing of personal data;
- authorising or denying requests for processing;
- receiving and investigating complaints about the misuse of personal data;
- conducting necessary inspections regarding personal data processing, and obtaining all information and documents needed;

- informing data controllers of alleged violations of the law and issuing mandatory measures for remedying these violations;
- imposing administrative sanctions on data controllers in the case of noncompliance;
- informing the public prosecutor of offenses committed under the law;
- keeping a public register of personal data processing operations;
- issuing public opinions on the state of data protection law;
- proposing amendments to simplify and improve data protection legislation, where necessary; and
- cooperating with international data protection authorities to share information and assistance, as well as participating in international negotiations.

Data controllers are required to file an annual report with the APDP concerning compliance with the processing.

REGISTRATION

The is no country-wide system of registration in the Republic of Benin. However, the law imposes an obligation of notification and requires the controller to keep a register of processing activities carried out under its responsibility.

Pursuant to Article 405 of the Digital Code, Automated or non-automated processing carried out by public or private bodies and involving personal data must, prior to their implementation, be the subject of a prior declaration to the Authority or be entered in a register kept by the person designated for that purpose by the controller.

All processing of personal data is subject to a reporting obligation to the Authority, except for the exemptions provided for in Book V of the Digital Code (see Articles 408, 410, 411, and 417 of the Digital Code).

In terms of Article 435 of the Digital Code, each controller and, where applicable, the controller's representative shall keep a register of the processing activities carried out under their responsibility.

This register shall include all of the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations;
- where applicable, transfers of personal data to a third country or to an international organization, including the identification of that third country or international organization;
- the time limits for the deletion of the different categories of data;
- a general description of technical and organizational security measures.

Each processor and, where applicable, the processor's representative of the processor shall also maintain a record of all categories of processing activities performed on behalf of the controller including:

- the name and contact details of the sub-processor(s) and of each controller on whose behalf the processor is acting and, where applicable, the names and contact details of the controller's or processor's representative and of the data protection officer;
- the categories of processing carried out on behalf of each controller;
- where applicable, transfers of personal data to a third country or to an international organization, including the identification of that third country or international organization and, in the case of transfers, the documents attesting to the existence of appropriate safeguards;
- a general description of the technical and organizational security measures.

The above-mentioned records must be in written form, including electronic form.

The controller or processor and, if applicable, their representative shall make the register available to the Authority upon request.

The obligation to keep a register does not apply to small and medium-sized enterprises except in the following cases:

- if the processing they carry out is likely to involve a risk to the rights and freedoms of the data subjects;
- if it is not occasional or if it concerns in particular the special categories of data referred to in article 394 paragraph 1 of the numerical code, or personal data relating to criminal convictions and offences.

DATA PROTECTION OFFICERS

According to the Article 430 of the Digital Code, a Data Protection Officer (DPO) must be appointed when the data controller is a state-owned organization or when the activities of the data controller or data processor involve monitoring individuals or processing of sensitive data on a large scale.

Although the Digital Code does not impose a strict duty for the appointment of a DPO, organizations with a DPO are exempt from notifying the APDP of data processing (Article 408 of the Digital Code).

COLLECTION & PROCESSING

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 383):

- processed lawfully, fairly and transparently;
- collected for specific, explicit, and legitimate purposes and not subsequently processed in a manner inconsistent with those purposes;
- processed appropriately, in a manner relevant and not excessive with regard to the purposes for which they are collected and processed;
- accurate and, if necessary, updated. All reasonable steps must be taken to ensure that inaccurate or incomplete data is erased or corrected;
- kept in a form that allows the identification of data subjects for a period not exceeding that necessary to achieve the purposes for which they are collected or for which they are processed;
- processed in a manner that ensures appropriate security of personal data

Notwithstanding the above, the overriding principle governing the processing of personal data in Benin is the prior consent of the data subject (see Articles 6 of the Data protection Law and 389 of the Digital Code.)

There are some exceptions to this principle. The prior consent of a data subject is not required when processing the data is meant to:

- comply with a legal obligation to which the controller is subject to;
- perform a task in the public interest or a task falling within the exercise of public authority, which is entrusted to the controller or the third party to whom the data are shared;
- perform a contract to which the data subject is a party or perform pre-contractual measures taken at the request of the data subject;
- protect fundamental interests or rights;
- perform certain activities in the framework of journalism, research or artistic or literary expression in compliance with the ethical rules of these professions.

When the processing is entrusted to a subcontractor, the controller or, where appropriate, his representative in the Republic of Benin, must:

- choose a subcontractor providing sufficient guarantees sufficient guarantees with regard to technical and organizational security and organizational measures relating to the processing;
- conclude a contract with the processor either in writing or via electronic means;
- define among other things the responsibility of the processor with regard to the data controller and their incumbent obligations in the privacy and security of the data

Under the applicable data protection law in Benin, individuals possess the following rights:

- right to obtain all their personal data in a clear format, as well as any available information as to their origin;
- right to withdraw consent for personal data processing at any time;
- the right to object, for lawful reasons, to the processing of their personal data;
- right to oppose the processing of their personal data for marketing purposes;
- right to rectify or erase personal data when it is deemed inaccurate or incomplete;
- right to not be subject to decisions made on the sole basis of an automated processing that would produce significant risks or harm;
- right to be forgotten, or to have information made public about themselves deleted from records; and
- right to obtain damages from data controllers when a breach occurs, leading to a material or non-pecuniary damage to a person.

Right to be informed

Data controllers must provide data subjects with information describing, among other things:

- the processing activities, such as data category;
- the purpose of processing;
- data recipients;
- the existence of profiling activities; and
- identification and contact details of the data controllers, or data subject rights.

Right to access

Any natural person whose personal data is processed may request from the controller information making it possible to know and contest the processing of their personal data, communication in intelligible form of data to personal character that concerns them as well as any available information as to their origin.

Right to rectification

Any natural person may require the data controller to correct, complete, update, block, or delete personal data concerning him, which is inaccurate, incomplete, ambiguous, out of date, or irrelevant, as the case may be, and as soon as possible, or whose collection, use, disclosure, or retention is prohibited. To exercise their right of rectification or deletion, the interested party sends a request, by post or electronically, dated and signed to the controller, or his representative.

Within 45 days following receipt of the request provided for in the previous paragraph, the controller communicates the rectifications or erasures of the data made to the data subject himself as well as to the persons to whom they are inaccurate, incomplete, equivocal, outdated, irrelevant or whose collection, use, communication, or storage is prohibited, have been communicated.

Right to erasure

See section above.

Right to object / opt-out

Any natural person has the right to object, at any time, for legitimate reasons, to the processing of personal data concerning him. It has the right, on the one hand, to be informed before data concerning it is communicated for the first time to third parties or used on behalf of third parties for purposes of prospecting, in particular commercial, charitable or political, and, on the other hand, to be expressly offered the right to oppose, free of charge, said communication or use.

Right to data portability

Data subjects have the right to receive the personal data concerning them that they have provided to a controller, in a structured, commonly used and machine-readable format, and have the right to transmit this data to another controller. processing without the controller to whom the personal data has been communicated obstructing it, when:

- the processing is based on consent or on a contract; and
- the processing is carried out using automated processes.

When the data subject exercises his right to data portability in application of the first paragraph, he has the right to obtain that the personal data are transmitted directly from one controller to another, when this is technically possible.

This right does not apply to processing necessary for the performance of a task of public interest or relating to the exercise of public authority vested in the controller. The right referred to in the first paragraph does not infringe the rights and freedoms of third parties.

TRANSFER

A personal data processor may transfer data to a foreign country if the receiving country ensures an adequate level of protection for the privacy and human rights and freedoms of the persons concerned.

The level of protection will be assessed according to:

- the data protection laws of the recipient country;
- the safety measures; and
- the processing characteristics (end, duration, nature, origin, destination of processed data).

It is worth noting that a country may not provide sufficient data protection, but if a recipient country is not deemed 'safe' in protecting data, but a data transfer is followed by protective measures such as contractual clauses or internal rules, assent could be provided by the APDP.

For instance, some data, such as biometric data, health data, data related to serious infringements, and data regarding crime, will be considered as involving specific risks for human rights and freedom of individuals' data. These data will need to be approved under Article 41 of the Law on the Protection of Personally Identifiable Information.

SECURITY

The Law on the Digital Code adopts a proportionate, context-specific approach to security.

Article 426 of this Law states that in order to guarantee the security of personal data, the controller and / or its processor must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, interception, in particular where the processing involves the transmission of data over a network, and against all other forms of unlawful processing.

These measures must ensure, taking into account the state of the art and the costs associated with their implementation, an appropriate level of security, taking into account, on the one hand, the state of the art in the field and the costs involved in applying these measures and, on the other hand, the nature of the data to be protected and the potential risks.

It is also the responsibility of the data controller, his representative and the sub-processor to ensure compliance with these security measures.

The Law on the Digital Code does require controllers and processors to consider the following when assessing what might constitute adequate security:

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

No specific requirements other than those set forth in the Law.

BREACH NOTIFICATION

A data controller must notify the Commissioner of the APDP of any breach to the security safeguards of personal data, without delay (Article 427 of The Law on the Digital Code).

The notification must, at a minimum:

- describe the nature of the security breach that affected personal data including, if possible, the categories and approximate number of individuals affected by the breach and the categories and approximate number of personal data records affected;
- provide the name and contact information of the Data Protection Officer or other point of contact from whom additional information can be obtained;
- describe the likely consequences of the security breach; and
- describe the steps taken or proposed to be taken by the controller to remedy the security breach, including, if applicable, steps to mitigate any adverse consequences.

Mandatory Breach Notification

Please refer to the comments above under Notification.

ENFORCEMENT

The data protection laws empower the authorities to impose various sanctions depending on the severity of the infringement. However, the level of enforcement remains quite low due to resource limitations and the fact that this field of law is still new to the administration and business and data subjects.

The Authority may issue a warning to a data controller who fails to comply with the obligations arising from the Digital Code. It may also give formal notice to the data controller to put an end to the non-compliance within a set period of time, which may not exceed eight (08) days.

The following constitute serious infringement of the Digital code:

- unfairly collecting personal data;
- communicating personal data to an unauthorized third party;
- collecting sensitive data, data relating to offences or to a notional identification number, without complying with the legal conditions;
- collect or use personal data in such a way as to cause a serious breach of fundamental rights or of the privacy of the individual concerned;
- prevent the Authority's services from carrying out an on-site inspection, or obstruct such an inspection.

Where the data controller fails to comply with the formal notice, the Authority may impose the following sanctions, in accordance with the principle of adversarial proceedings:

- a pecuniary penalty, except in cases where processing is carried out by the State;
- an injunction to cease processing personal data;
- a final or temporary withdrawal of the authorization granted in application of the provisions of the Digital Code;
- blocking of certain personal data.

The amount of the fine is proportionate to the seriousness of the breaches committed and to the benefits derived from the breach.

For the first breach, it may not exceed XOF fifty million (50,000,000). In the event of repeated breaches within five (05) years of the date on which the penalty previously imposed became final, it may not exceed XOF one hundred million (100,000,000) or, in the case of a company, five percent (5%) of sales excluding tax for the last financial year closed, up to a maximum of XOF one hundred million (100,000,000).

Where the Authority has imposed a fine that has become final before the criminal court has given a final ruling on the same or related facts, the latter may order that the fine be deducted from the fine imposed.

Sanction by the data protection Authorities may be appealed before the competent administrative court.

ELECTRONIC MARKETING

The personal data Act will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name).

The general rule for electronic marketing is that it requires the express consent of the recipient (see Article 245 of the Law No. 2017-20 of April 20, 2018 on the digital code in the Republic of Benin).

Even when a marketer has the consent of a data subject, that consent can be withdrawn by the data subject under Article 334 of the Law No. 2017-20 of April 20, 2018 on the digital code in the Republic of Benin.

The data subject has the right to object at any time to the use of his / her personal data for such marketing.

This right to object must be explicitly brought to the attention of the data controller.

However, the data controller may not respond favorably to a request to exercise the right to object if it demonstrates the existence of legitimate reasons justifying the processing, which override the interests, fundamental rights and freedoms of the data subject.

ONLINE PRIVACY

Not applicable.

KEY CONTACTS

Geni & Kebe
www.dlapiperafrica.com/senegal

Dr. Sangare Mouhamoud
Associate
Geni & Kebe
T +2250779107541
m.sangare@gsklaw.sn

Dr. Francky Lukanda
Senior Associate
Geni & Kebe
T +2250584344660
f.lukanda@gsklaw.sn

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BERMUDA

Last modified 28 January 2024

LAW

The Bermuda legislature passed a comprehensive legislative framework that specifically addresses issues of data protection in the form of the Personal Information Protection Act 2016 (PIPA). The principal provisions of PIPA will come into force on 1 January 2025.

Apart from PIPA, Bermuda law recognizes a duty of confidentiality in certain circumstances under the common law.

DEFINITIONS

Definition of use

PIPA applies to the "use" of personal information, and defines "use" as carrying out any operation on personal information, including collecting, obtaining, recording, holding, storing, organising, adapting, altering, retrieving, transferring, consulting, disclosing, disseminating or otherwise making available, combining, blocking, erasing or destroying it.

Definition of personal data

PIPA provides for a definition of "personal information" as meaning "any information about an identified or identifiable individual".

At common law, information is generally to be regarded as 'confidential' if it has a necessary quality of confidentiality and has been communicated or has become known in such circumstances as give rise to a reasonable expectation of confidence; for example if obtained in connection with certain professional relationships, if obtained by improper means, or if received from another party who is subject to a duty of confidentiality.

Definition of sensitive personal data

PIPA provides for a definition of "sensitive personal information" as meaning "any personal information relating to an individual’s place of origin, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information".

NATIONAL DATA PROTECTION AUTHORITY

Alexander White, a US lawyer, has been the appointed Privacy Commissioner since 20 January 2020. He is responsible for setting up the Privacy Commissioner's Office, hiring and training staff, undertaking investigations, providing reports and developing public awareness of the rights of individuals and the obligations of organisations under PIPA.

REGISTRATION

There is no system of registration and none provided for in PIPA.

DATA PROTECTION OFFICERS

There is currently no requirement to appoint a data protection officer. Once PIPA is fully in force, organisations covered by the legislation will be required to appoint a "privacy officer" for the purposes of compliance with PIPA.

COLLECTION & PROCESSING

Once fully in force, PIPA will regulate the collection and processing of personal information and will apply to any individual, entity or public authority collecting, storing and using personal information in Bermuda either electronically or as part of a structured filing system. The use to which sensitive personal information can be put by an organisation is much more restrictive.

The common law, which will continue to apply in parallel with PIPA, will in certain cases consider it a breach of confidence to misuse or threaten to misuse confidential information. The concept of 'misuse' is a broad one, but will often include any unauthorised disclosure, examination, copying or taking of confidential information. The precise scope of the term however will depend largely on the specific circumstances, including the relevant relationship and the nature of the information.

TRANSFER

Once fully in force, PIPA will regulate the transfer of personal information to an overseas third party. The legislation provides that the Privacy Commissioner can designate jurisdictions as providing comparable protection to Bermuda law. In other cases, the organisation subject to PIPA will be required to employ contractual mechanisms, corporate codes of conduct or other means to ensure that the overseas third party provides comparable protection for the personal information.

SECURITY

Once fully in force, PIPA will make provision for the implementation of proportional security safeguards against risk including loss, unauthorised access, destruction, use, modification or disclosure. In addition, a person who misuses or divulges confidential information (deliberately or otherwise) may be liable at common law.

BREACH NOTIFICATION

Once fully in force, PIPA will require notification of a breach of security leading to the loss or unlawful destruction or unauthorised disclosure of, or access to, personal information which is likely to adversely affect an individual to (a) the individual concerned; and (b) the Privacy Commissioner.

The notice to the Commissioner must describe the nature of the breach, its likely consequences for the individual concerned, and the measures the organisation is taking to address the breach.

ENFORCEMENT

Once fully in force, PIPA will make provision for investigations and inquiries by the Privacy Commissioner and for a range of remedial orders that may be imposed by the Commissioner. It also provides for a claim for compensation for financial loss or emotional distress for failure to comply with the legislation (subject to a reasonable care defence). In addition, PIPA makes provision for criminal offences and penalties (including imprisonment) for misuse of personal information. In addition, a breach of the common law duty of confidentiality may give rise to a claim for, among other things, damages and/or an injunction. These remedies are to be sought through, and enforced by, the Bermuda courts.

An individual convicted of an offence under PIPA will be liable to a fine of up to BMD 25,000 and/or to imprisonment for up to two years. An organisation convicted of an offence under PIPA will be liable to a fine of up to BMD 250,000. Proceedings can be brought against company directors and other officers in a personal capacity.

ELECTRONIC MARKETING

The Electronic Transactions Act 1999 provided that the Minister responsible for electronic commerce had the power to issue a standard to apply to intermediaries or e-commerce service providers and such a standard was issued by the Minister on 5 May 2000 and came into force on 3 July 2000 (Standard). The definition of "e-commerce service provider" is "a person who uses electronic means in providing goods, services or information" while an "intermediary" (with respect to an electronic record) means "a person who, on behalf of another person, sends, receives or stores that electronic record or provides other services with respect to that electronic record". The Standard set out certain "Safe Harbour Guidelines" which included certain privacy requirements and the prohibition on the sale or transfer of personal data or business records of customers to another person for the purposes of sending bulk, unsolicited electronic records.

ONLINE PRIVACY

Once fully in force, PIPA will make special provision based on parental consent for certain uses of personal information about a child under the age of 14. Subject to this, there are no specific restrictions addressing online privacy of confidential information beyond those generally applicable to the use of confidential information.

KEY CONTACTS

Carey Olsen
www.careyolsen.com/

Michael Hanson
Managing Partner
Carey Olsen
T +1 441 542 4501
michael.hanson@careyolsen.com

Keith Robinson
Partner
Carey Olsen
T +1 441 542 4502
keith.robinson@careyolsen.com

Jay Webster
Partner
Carey Olsen
T + 1 441 542 4517
jay.webster@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BOLIVIA

Last modified 24 January 2022

LAW

- Bill of Personal Data Protection;
- The Political Constitution of the Plurinational State of Bolivia, in Article N°130.

Any individual or collective person who believes to be unduly or illegally prevented from knowing, objecting or obtaining the deletion or rectification of the data registered by any physical, electronic means, magnetic or computer, in public or private files or databases, or that affect their fundamental right to personal or family privacy, or in their own image, honor and reputation, may file a Private Protection Action.

DEFINITIONS

Definition of personal data

Any information about a natural person identified or identifiable, expressed by numbers, alphabetic letters, graphics, photographs, alphanumeric symbols, acoustic forms or any other type of data. It is considered that a person is identified when his identity can be determined directly or indirectly as long as this do not require terms or disproportionate activities.

Definition of sensitive personal data

Data that refers to the intimate sphere of the individual, or whose inappropriate use can cause discrimination of any type or high risk to the particular individual.

NATIONAL DATA PROTECTION AUTHORITY

The Personal Data Authority, is the Agency of the electronic government and information technologies and communication (AGETIC).

REGISTRATION

It is not established in the Bill of Personal Data Protection, in a prescriptive manner, however, it establishes that personal data can only be processed with the **consent of its owner**, unless it is by court order issued for reasons of public interest. It is not yet established whether entities or persons interested in the personal data of a third party must request authorization from the Personal Data Protection Authority.

DATA PROTECTION OFFICERS

The President of the Personal Data Authority is the principal officer and has an Executive Council with three members:

- the general Director of the electronic government and information technologies and communication Agency; and

- two designated members from the Ejecutive Council.

The Ejecutive Council of the Personal Data Protection Authority will be assisted by a Consultive Council integrated by six members:

- a person with human rights experience;
- a judicial organ representative;
- an electoral organ representative;
- a Public Ministry representative;
- an academic area representative; and
- a private sector representative.

COLLECTION & PROCESSING

Under the legitimation principle, the person responsible within the Personal Data Protection Authority may only process personal data when the owner grants his consent for one or more specific purposes, when necessary for the fulfilment of a court order, for the defence or recognition of the rights of the holder/owner before a public authority, to protect the vital interests of the holder/owner or of another natural person; among other legitimate and informed reasons.

TRANSFER

Nothing in the Bill of Personal Data Protection is established concerning transfer.

SECURITY

The person responsible for the personal data bank must adopt technical, organizational and legal measures that guarantee its security and prevents its alteration, loss, treatment or unauthorized access.

The requirements and conditions that personal data banks must meet regarding security are established by the National Authority for the Protection of Personal Data, except for the existence of special provisions contained in other laws.

The processing of personal data in data banks that do not meet the requirements and security conditions is prohibited.

BREACH NOTIFICATION

When the person in charge is aware of a breach of security of personal data that occurs at any stage of the treatment, understood as any damage, loss, alteration, destruction, access, and in general, any illegal or unauthorized use of personal data even when it occurs accidentally, it will notify the control authority and the affected owners of such suffering immediately.

The foregoing will not be applicable when the person in charge can prove, according to the principle of proactive responsibility, the impossibility of the security breach that has occurred, or, which does not represent a risk to the rights and freedoms of the owners involved.

The notification made by the person responsible to the affected owners will be written in a clear and simple language.

The notification should contain at least the following information:

- the nature of the incident;
- the Personal data compromised;
- coercive actions carried out immediately;
- recommendations to the holder about the measures that can help protect their interests; and
- the means available to the holder to obtain more information.

The person responsible shall document any breach of the security of the data that occurred at any stage of the treatment, identifying, but not limited to, the date on which they discovered the reason for the breach, the related facts, their effects and the corrective measures implemented immediately and definitively, which will be available to the supervisory authority.

The Regulation on the Right to Protection of Personal Data contemplates the effects of the notifications of security breaches made by the person in charge of the Control Authority in regard to the procedures, form and conditions of its intervention in order to safeguard the interests, rights and freedoms of the affected owners.

There is no mandatory breach notification requirement under the Data Protection Law.

ENFORCEMENT

The competent authority for the enforcement of Data Protection Law is the Personal Data Authority, the Agency of the electronic government and information technologies and communication (AGETIC). However, considering that Authority is not yet created, the level of enforcement may be distributed to other legislative organs in the future.

ELECTRONIC MARKETING

There is nothing legally established in Bolivia concerning electronic marketing.

ONLINE PRIVACY

There is nothing established about online privacy, or cookies, or location data.

KEY CONTACTS

Guevara & Gutierrez
gg-lex.com/

Marcos Mercado Delgadillo
Guevara & Gutierrez
mmercado@gg-lex.com

Jorge Luis Inchauste Comboni
Guevara & Gutierrez
jinchauste@gg-lex.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BONAIRE, SINT EUSTATIUS AND SABA

Last modified 28 January 2024

LAW

- **Personal Data Protection Act BES** *(Wet bescherming persoonsgegevens BES)* (“Personal Data Protection Act BES”);
- **General Data Protection Regulation** (the “GDPR”) – a regulation of the European Union which became effective on May 25, 2018.

DEFINITIONS

Definition of Personal Data

Personal Data Protection Act BES

Article 1 paragraph 2 of the Personal Data Protection Act BES stipulates personal data as any data concerning an identified or identifiable natural person.

GDPR

Personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Definition of Sensitive Personal Data

Personal Data Protection Act BES

A person’s religion or belief, race, political views, health, sexual life as well as personal data concerning membership of a trade union.

GDPR

Data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

NATIONAL DATA PROTECTION AUTHORITY

Personal Data Protection Act BES

The Personal Data Protection Committee as referred to in article 44 of Personal Data Protection Act BES.

GDPR

An independent public authority established by a Member state pursuant to article 51 of the GDPR (Article 4(21), GDPR). The authority is responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the EU.

REGISTRATION

Personal Data Protection Act BES

No registration required.

GDPR

Article 30 GDPR requires companies to keep an internal electronic registry, which contains the information of all personal data processing activities carried out by the company.

DATA PROTECTION OFFICERS

Personal Data Protection Act BES

Pursuant to article 13 of the Personal Data Protection Act BES the responsible party shall execute appropriate technical and organizational measures to secure personal data against loss or any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking account of the technical state of the art and the costs of execution, in view of the risks associated with that processing and the nature of the data to be protected. The measures shall be aimed partly at preventing unnecessary gathering and further processing of personal data.

Besides the measures above, the Personal Data Protection Act BES does not contain any clauses on any type of registration, filings of documents to any public agency or having a mandatory data protection officer in place.

GDPR

The appointment of a data protection officer under the GDPR is only mandatory in three situations:

- When the organisation is a public authority or body;
- If the core activities require regular and systematic monitoring of data subjects on a large scale; or
- If the core activities involve large scale processing of special categories of personal data and data relating to criminal convictions.

COLLECTION & PROCESSING

Personal Data Protection Act BES

Collecting and processing: any act or set of acts relating to personal data, including in any case the collection, recording, organization, storage, updating, modification, retrieval, consultation, use, disclosure by transmission, dissemination or any other form of making available, bringing together , as well as data blocking, erasure or destruction of data.

GDPR

Collection: a natural or legal person, public authority, agency or other body that collect personal data and use it for certain purposes, like a website that markets to users based on their online behaviour.

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority.

TRANSFER

Personal Data Protection Act BES

Article 42 of Personal Data Protection Act BES stipulates that personal data that is subject to processing or that are intended to be processed after its transfer may only be transferred to a country outside the European Union if, without prejudice to compliance with the law, that country guarantees an adequate level of protection.

GDPR

The GDPR restricts transfers of personal data outside the European Economic Area, or the protection of the GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.

SECURITY

Personal Data Protection Act BES

Pursuant to article 13 of the Personal Data Protection Act BES the responsible party shall execute appropriate technical and organizational measures to secure personal data against loss or any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking account of the technical state of the art and the costs of execution, in view of the risks associated with that processing and the nature of the data to be protected. The measures shall be aimed partly at preventing unnecessary gathering and further processing of personal data.

GDPR

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (article 32 GDPR).

BREACH NOTIFICATION

Personal Data Protection Act BES

Contains no specific clauses.

GDPR

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with article 55 GDPR, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

ENFORCEMENT

Personal Data Protection Act BES

Pursuant to the Personal Data Protection Act BES the committee is authorized to impose an order under administrative coercion to enforce the obligations laid down by or pursuant to the Personal Data Protection Act BES.

GDPR

The GDPR holds a variety of potential penalties for businesses.

For example, article 77 of GDPR states that:

“Every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating him or her infringes this Regulation.”

Additionally, article 79 of the Regulation states that *“such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence.”*

Penalties

Compensation to Data Subjects. One penalty that may be imposed is compensation to, as stated in article 82 of the Regulation, *“Any person who has suffered material or non-material damage as a result of an infringement of this Regulation”* for the damage they’ve suffered.

Fines

Article 83 of GDPR specifies a number of different fines that may vary based on the nature of the infraction, its severity, and the level of cooperation that “data processors” (i.e. you) provide to the “supervisory authority.” Less severe infringements may incur administrative fines of up to 10,000,000 Euros or 2% of your total worldwide annual turnover for the preceding year (whichever is greater), while more severe infractions may double these fines (20,000,000 or 4% annual turnover).

Individual Member States of the EU may have additional fines and penalties that may be applied as well. However, these additional penalties are not specifically listed in the text of the Regulation since they’re up to the individual EU nations to set— the only guidelines in article 84 of GDPR are that *“Such penalties shall be effective, proportionate and dissuasive”* and that *“Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018.”*

ELECTRONIC MARKETING

Personal Data Protection Act BES

N/A.

GDPR

Under article 22 GDPR organizations cannot send marketing emails without active, specific consent.

Companies can only send email marketing to individuals if:

- The individual has specifically consented.
- They are an existing customer who previously bought a similar service or product and were given a simple way to opt out.

ONLINE PRIVACY

Personal Data Protection Act BES

Contains no specific clauses.

GDPR

Cookies, insofar as they are used to identify users, qualify as personal data and are therefore subject to the GDPR. Companies do have a right to process their users’ data as long as they receive consent or if they have a legitimate interest.

Location data, the GDPR will apply if the data collector collects the location data from the device and if it can be used to identify a person.

If the data is anonymized such that it cannot be linked to a person, then the GDPR will not apply. However, if the location data is processed with other data related to a user, the device or the user’s behavior, or is used in a manner to single out individuals from others, then it will be “personal data” and fall within the scope of the GDPR even if traditional identifiers such as name, address etc. are not known.

KEY CONTACTS

HBN Law & Tax
hbnlawtax.com/

Maarten Willems
Senior Associate
HBN Law & Tax
T +297 588 6060
maarten.willems@hbnlawtax.com

Misha Bemer
Partner
HBN Law & Tax
T +297 588 6060
misha.bemer@hbnlawtax.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BOSNIA AND HERZEGOVINA

Last modified 21 December 2022

LAW

The Law on Protection of Personal Data ('Official Gazette of BIH', nos. 49/06, 76/11 and 89/11) (DP Law) is the governing law regulating data protection issues in Bosnia and Herzegovina (BiH). The DP Law came into force on July 4, 2006 and was amended on October 3, 2011.

Due to the deficiencies and non-alignment of the DP Law with the GDPR, in 2018, the competent authorities initiated the procedure for adoption of a new GDPR compliant data protection law in BiH. According to the publicly available information the draft of the new data protection law (Draft Data Protection Law), was forwarded to the BiH Ministry of Civil Affairs and the adoption procedure before the BiH Parliament should have been initiated. However, due to the complex political the Draft Data Protection Law is not adopted to date. However, we expect the Draft Data Protection Law to be adopted in its current text within the following year.

DEFINITIONS

Definition of personal data

The DP Law defines personal data as any information relating to an identified or identifiable natural person. Data subjects are natural persons whose identity can be determined or identified, directly or indirectly, in particular by reference to a personal identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

The DP Law defines sensitive personal data as any data relating to any of the following:

- Racial, national or ethnic origin;
- Political opinion, party affiliation, or trade union affiliation;
- Religious, philosophical or other belief;
- Health;
- Genetic code;
- Sexual life;
- Criminal convictions; and
- Biometric data.

Definitions of sensitive personal data stipulated by Draft Data Protection Law correspond to the definitions prescribed by GDPR.

NATIONAL DATA PROTECTION AUTHORITY

The Personal Data Protection Agency (DPA) is the national data protection authority in BiH. The DPA is seated in:

Dubrovačka 6
Sarajevo
www.azlp.ba

The DPA remains national data protection authority under Draft Data Protection Law.

REGISTRATION

Each data controller (defined as a person or legal entity which processes personal data) must provide the DPA with specific information on the database containing personal data ("**Database**") established and maintained by the controller. The DPA maintains a publicly available register of data controllers and Databases.

The Database's registration includes two phases:

- First, the controller must register as a data controller (this registration as a controller is to be performed only once).
- Second, the controller must report to the Database's establishment, which has to be done within 14 days.

Registration of the Database is made by submitting the application in the prescribed form to the DPA. The DPA form includes information regarding:

- Data controller
  - Name
  - Address of its registered seat
- The Database itself
  - Processing purpose
  - Legal ground for its establishment
  - Identification of exact processing activities
  - Types of processed data
  - Categories of data subjects, and
  - Transfer of data abroad

If there is a subsequent change in the registered data, for example changing initial processing activities, the change needs to be reported to the DPA within 14 days from the date the change occurred.

Unlike the DP Law, the Draft Data Protection Law foresees the obligation of data controllers and data processors to keep records of their data processing activities identically as the GDPR, however it does not oblige data controllers to register their data processing activities/databases with the Agency.

DATA PROTECTION OFFICERS

There is no statutory obligation that the entity which processes personal data has a data protection officer. The Rules on the Manner of Keeping and Special Measures of Personal Data Technical Protection (Official Gazette of BiH no. 67/09) (Rules) stipulate that a controller can have an administrator of the Database. Such administrator is a natural person authorized and responsible for managing the Database and ensuring privacy and protection of personal data processing, in particular regarding implementation of security measures, storage and protection of data.

Unlike DP Law, the Draft Data Protection foresees the obligation of data controller and processor to ensure properly and timely involvement of the data protection officer in all issues related to the protection of personal data. Position and tasks of data protection officer envisaged by Draft Data Protection Law correspond to those prescribed by GDPR.

COLLECTION & PROCESSING

Collection and processing of personal data is permissible if carried out pursuant to the data subject’s consent and in compliance with the basic principles of personal data protection.

The form of the data subject’s consent depends on the type of personal data collected and processed. While the collection and processing of sensitive personal data requires explicit written consent from the data subject, the consent for the collection and processing of personal data falling within a category of general personal data does not have to be in writing. However, at the request of the competent authority, the controller has to be able to prove, at any time, the existence of a data subject’s consent for processing of both personal and sensitive personal data. Therefore, having a written consent for collection of any personal data is advisable. When required, written consent must contain at minimum elements prescribed by the DP law.

Apart from the consent, there are also other conditions which must be met for the collection and processing to be regarded as legitimate, including:

- Processing must be done in a fair and lawful way;
- The type and scope of processed data must be proportionate to the respective purpose; and
- Other principles regarding the legitimate reasons for personal data processing.

The DP Law provides an exception when a data subject's personal data may be processed without the data subject’s consent. This is the case where the processing is necessary for the fulfillment of a data controller’s statutory obligations or for preparation or realization of an agreement concluded between a data controller and a data subject (Exceptional Cases). These conditions are considered the basic principles of personal data protection and are applicable to each case of personal data processing.

The legal grounds as well as the data processing requirements envisaged by the Draft Data Protection Law fully correspond to those envisaged by the GDPR.

TRANSFER

Under the transfer rules set out in the DP Law, processed personal data may be transferred to countries where an adequate level of personal data protection is ensured. In that regard, preferential status is given to the member states of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("**Convention**"), as members of the Convention ensure an adequate level of personal data protection.

Personal data transfer to countries that do not provide for an adequate level of personal data protection is allowed in certain cases stipulated by the DP Law, for example:

- When the data subject consented to the transfer and was made aware of possible consequences of such transfer;
- When it is required for the purpose of fulfilling the contract or legal claim; or
- When it is required for the protection of public interest.

In addition, the DPA may exceptionally approve the transfer to a country that does not ensure adequate an level of personal data protection if the controller in the country where the data is to be transferred can provide for sufficient guarantees in regard to the protection of privacy and fundamental rights and freedoms of the data subject.

The Draft Data Protection Law prescribes a set of mechanisms based on which a legitimate transfer of data out of BiH is possible. This means that the Draft Data Protection Law tends, the same as the GDPR, to enable legitimate transfer of personal data whenever there are some safeguards that transferred data will be processed in line with the law.

Aforementioned means the following:

- It should firstly be checked whether a particular country to which the data is to be transferred is regarded as a country with an adequate data protection system (“**Adequate Country**”);
- If a country to which the data is to be transferred from BiH is the Adequate Country or if there is a data transfer related international treaty entered into between BiH and that country, a transfer is possible without any approval of the Agency (“**Transfer Approval**”);
- On the other hand, if a country to which the data is to be transferred is not the Adequate Country, a transfer is still possible without the Transfer Approval if the adequate data protection measures are undertaken (e.g., if appropriate

standard contractual clauses have been entered into between a data exporter and a data importer) (“**Adequate Safeguards**”);

- However, even if there are no Adequate Safeguards, there is still a possibility for transferring the data without the Transfer Approval. Such possibility exists in so-called special situations, explicitly prescribed by the Draft Data Protection Law, the same as under the GDPR (e.g., a data subject has consented to a particular transfer, a transfer is necessary for the realization of an agreement between a data subject and data controller, etc.);
- Finally, even if none of the aforementioned special situations is applicable, a data transfer is still allowed without the Transfer Approval if certain conditions (linked to a data controller's legitimate interest) explicitly prescribed by the Draft Data Protection Law are cumulatively fulfilled.

SECURITY

The DP Law requires data controllers and processors to:

- Take care of data security and to undertake all technical and organizational measures;
- Undertake measures against unauthorized or accidental access to personal data, their alteration, destruction or loss, unauthorized transfer, other forms of illegal data processing, as well as measures against misuse of personal data; and
- Adopt a personal data security plan ("**Security Plan**") which specifies technical and organizational measures for the security of personal data.

As provided by the Rules (as defined in the section "**Data Protection Officers**"), the Security Plan includes the categories of processed data and the list of instruments for protection of the data to ensure confidentiality, integrity, availability, authenticity, possibility of revision and transparency of the personal data.

The Rules prescribe that the controller is required to undertake more stringent technical and organizational measures when processing sensitive personal data. Such measures aim at enabling recognition of each authorized access to the information system, operation with the data during the controller’s regular working hours and cryptographic protection of the data transmission via telecommunications systems with appropriate software and technical measures.

The Rules also closely regulate the manner of personal data keeping and personal data protection in automatic processing.

Security measures envisaged by Draft Data Protection Law correspond to the measures prescribed by GDPR.

BREACH NOTIFICATION

The DP Law does not impose data security breach notification duty on the controller. However, the Rules do impose a duty on the Database's administrator, processor and performer to inform the controller on any attempt of unauthorized access to information system for the Database's management.

However, the regulations issued by the Communication Regulatory Agency (RAK) should be considered. The Regulation on Carrying out the Activities of the Publicly Available Electronic Communication Networks ('Official Gazette of BiH' no. 66/12) (Regulation A) stipulates that the operator of publicly available electronic communication networks (Operator) is required to inform RAK about its activities, operations and other applicable information required for RAK’s regulatory competences. Since RAK’s Regulation on Conditions for Providing the Telecommunications Services and Relation with End Users ('Official Gazette of BiH' no. 28/13) (Regulation B) prescribes for the Operator’s obligation to undertake such methods which will protect the privacy of users and others, in a manner that will ensure the integrity and confidentiality of data, it can be concluded that the Operator is required to notify RAK of any breach of security and integrity of public telecommunication services that resulted in violation of protection of personal data or privacy of the respective services' s users.

When it comes to the notification duty towards the users, the Regulation B obliges the Operator to inform the users adequately (e.g. in user agreement, in its terms and conditions or in the appropriate technical way) about the possibility of privacy or telecommunication facilities violations.

Pursuant to the Draft Data Protection Law in case of a personal data breach the controller is obliged to undue delay and where feasible not later than 72 hours after having become aware of it, which fully correspond to the obligation prescribed by GDPR.

ENFORCEMENT

The DPA enforces the DP Law. The DPA is authorized and obliged to monitor implementation of the DP Law, both *ex officio*, and upon a third-party complaint. If the DPA finds that a particular person or entity processing personal data acted in violation of data processing rules, it may request that the controller discontinue such processing and order specific measures to be carried out without delay.

When acting upon the complaints, the DPA may also issue a decision by which it can order blocking, erasing or destroying of data, adjustment or amendment of data, temporary or permanent ban of processing, issue warning or reprimand to the controller. The decision of the DPA may not be appealed; however, a party may initiate administrative dispute before the Court of BiH.

The DPA can initiate a misdemeanor proceeding against the respective data controller before the competent court, depending on the gravity of the particular misconduct and the data controller’s behavior with respect to the same. The offenses and sanctions are explicitly prescribed by the DP Law, which includes monetary fines for a controller in the amount between € 2,550 and €51,100, as well as for the controller's authorized representative in the amount between €100 and €7,700.

The Draft Data Protection Law, although still not as strict as the GDPR, foresees fines which are significantly higher than the ones foreseen by the Current Data Protection Law. Specifically, the Draft Data Protection Law introduces fines in the amount of up to BAM 200,000 (approx. EUR 100,000) or 4% of the total worldwide annual turnover of the preceding financial year (whichever is higher).

Breach of personal data protection regulations represents a criminal offense of unauthorized collection of personal data by all criminal codes applicable in BiH (Criminal Code of BiH, Criminal Code of the Republic of *Srpska*, Criminal Code of the Federation of BiH and Crimes Code of *Brčko Distrikt*). Prescribed sanctions are monetary fines (in amount to be determined by the court) or imprisonment up to six (6) months (Criminal Code of BiH; Criminal Code of the Federation of BiH; Criminal Code of the *Brčko Distrikt*) or up to one (1) year (Criminal Code of the Republika *Srpska*).

ELECTRONIC MARKETING

Although electronic marketing is not governed by the DP Law, the respective law regulates protection of personal data used in direct marketing. In that regard, the controller is not allowed to disclose personal data to a third party without the data subject’s consent. However, when that is necessary for the protection of the controller’s rights and interests and when it is not in contradiction with the data subject’s right to the protection of personal privacy and personal life, the personal data may be used for direct marketing purposes without consent. The DPA is of the opinion that previous provision could be used only in explicit cases, when the controller is offering products or services to regular client in order to limit possible future damages for which he could be held responsible.

Under Regulation B, the Operator is prohibited from using user personal data for purposes of its business or other promotions, unless it obtains explicit consent from the user to whom such data relates.

ONLINE PRIVACY

The general data protection rules, as introduced by the DP Law, are relevant for online privacy as well, as there are no specific regulations that explicitly govern online privacy. This includes obligation to act in accordance with the basic principles of personal data protection set out in the DP Law as well as acting on the basis of the data subject's informative consent.

KEY CONTACTS

Karanovic & Nikolic
www.karanovic-nikolic.com/

Nihad Sijercic

Attorney-at-law in cooperation with Karanovic & Partners
T +387 33 844 000
nihad.sijercic@karanovicpartners.com

Amina Dugum
Attorney-at-law in cooperation with Karanovic & Partners
T +387 33 844 000
amina.djugum@karanovicpartners.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BOTSWANA

Last modified 12 January 2023

LAW

The Data Protection Act – Act No. 32 of 2018, (“the DPA”) is an Act which was assented to by Parliament on the 3rd August 2018 and came into effect on the 15th of October 2021.

The DPA regulates the protection of personal data and ensure that the privacy of individuals in relation to their personal data is maintained.

DEFINITIONS

Definition of personal data

Under the DPA, personal data means information relating to an identified or identifiable individual, which the individual can be identified directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to the individual’s physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

Sensitive Personal Data is defined to mean personal data which reveals a data subject’s:

- racial or ethnic origin;
- political opinions;
- religious beliefs or philosophical beliefs;
- membership of a trade union;
- physical or mental health or condition;
- sexual life;
- filiation; or
- personal financial information,

and includes:

- any commission or alleged commission by him or her of any offence;
- any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings, or the sentence of any Court in such proceedings; and
- genetic data, biometric data and the personal data of minors.

NATIONAL DATA PROTECTION AUTHORITY

A body known as the Information and Data Protection Commission (“**the Commission**”) as established under the DPA has been formed and is the designated body tasked with data protection and ensuring the effective application of, and

compliance with the DPA, and in particular, the right to protection of personal data, access rectification, objection and cancellation of such data.

REGISTRATION

The Commission is responsible for creating and maintaining a public register of all data controllers. There is, however, currently no prescribed method of registration.

A data controller is a person who alone or jointly with others determines the purposes and means of which personal data is to be processed, regardless of whether or not such data is processed by such person or agent on that person's behalf. Additionally, a data controller may engage a data processor, being a person who processes data on behalf of the data controller.

In terms of the DPA, data controllers are required to notify the Commissioner of the Commission (“**the Commissioner** ”) before carrying out any wholly or partially automated processing operation or set of such operations which are intended to serve a single purpose or serve several related purposes.

The notification should include the following details:

- The name and address of the data controller or data processor;
- The purpose of the processing;
- A description of the category or categories of a data subject and of the personal data or categories of personal data relating to the data subject;
- The recipients to whom personal data can be disclosed to;
- Proposed transfers of personal data to a third country; and
- A general description to allow the Commission to preliminarily assess the appropriateness of the security measures.

The requirement for notification does not apply to operations which have the sole purpose of keeping a register that is intended to provide information to the public by virtue of any law, and for which the register is open for public inspection. In addition, the notification will not be required where a data controller has appointed a data protection representative.

Data controllers are further required to immediately notify the Commissioner of any breach to the technical or organizational security safeguards for processing of personal data.

The Commissioner has the authority to grant an exemption for notification when satisfied that:

a. The personal data being processed has no apparent risk of infringement to the rights of the data subject;
b. The purposes of the processing, the category of processing, the category of a data subject, the category of a recipient, and the data retention period are specified; and
c. The data controller has appointed a data protection representative, and the Commissioner has been notified of such appointment.

DATA PROTECTION OFFICERS

A data controller has the option to appoint a data protection representative who holds the requisite qualifications, their role being to independently ensure that personal data is processed in a correct and lawful manner, and in accordance with good practice.

The data protection representative is responsible for keeping a list of the processing carried out and the list should be immediately accessible to any person applying for access. Upon identifying any inadequacies, the data protection representative should bring such inadequacies to the attention of the data controller and assist in ensuring that the data subject’s rights under the DPA are protected.

Where a data protection representative has been appointed, the notification to the Commissioner regarding wholly or partially automated processing operations is not required.

If a data protection representative has reason to suspect that the data controller is contravening the rules applicable for processing personal data, and if rectification is not implemented as soon as practicable after the contravention is pointed out, the data protection representative must then notify the Commissioner.

The appointment and removal of a data protection representative must be notified to the Commissioner.

COLLECTION & PROCESSING

Processing means any operation or a set of operations which is taken in regard to personal data, whether or not it occurs by automatic means, and includes the collection, recording, organization, storage, alteration, retrieval, gathering, use, disclosure by transmission, dissemination or otherwise making information available, alignment, or combination, blocking, erasure or destruction of such data.

Processing personal data

Prior to undertaking the processing of personal data, data controllers are generally required to obtain written consent from the data subjects. Consent is not required in instances authorised by any written law. In addition, a data subject who has given consent for processing of personal data may at any time, in writing, revoke the consent for legitimate, reasonable, and compelling reasons at that particular time.

Alternatively to where written consent is obtained, personal data may further be processed where the processing is necessary for:

- the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject entering into a contract;
- compliance with a legal obligation to which the data controller is subject;
- protecting the vital interests of the data subject;
- performing an activity that is carried out in the public interest or in the exercise of an official authorization vested in the data controller, or of a third party to whom the data is disclosed; or
- a purpose that concerns a legitimate interest of the data controller, or of a third party to whom personal data is provided, except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject and in particular, the right to privacy.

Where personal data is processed for historical, statistical or scientific purposes, the data controller must ensure that there are appropriate security safeguards in place in instances where the personal data may be kept for a period longer than necessary, having regard to the purpose for which it is processed or the personal data kept is not used for any decision concerning the data subject.

In the event that processing is for direct marketing, the data controller must, at no cost, inform the data subject of the right to oppose the processing. Processing for such purposes will be prohibited where the data subject has given a notice of objection to the processing of the personal data. A data controller who processes the data despite the objection made by the data subject commits an offence which is punishable by fine not exceeding BWP500 000 or to imprisonment for a term not exceeding nine years, or to both.

Processing sensitive personal data

Processing sensitive personal data is heavily restricted thereby requiring the data controller to ensure that appropriate security safeguards have been adopted. The processing of sensitive personal data is generally be prohibited save for where:

- the processing is specifically provided for under the DPA;
- the data subject has given consent in writing;
- the data subject has made the data public;

- the processing is necessary for national security, for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment, or where the processing is authorized by any other written law for any reason of substantial interest to the public; or
- the processing is necessary to protect the vital interest of a data subject and another person in a case where consent cannot be given by or on behalf of the data subject, the data controller cannot be reasonably expected to obtain consent or the consent by or on behalf of the data subject has been unreasonably withheld.

Bodies or entities, not being a commercial bodies or entities, which have political, philosophical, religious or trade union objects are allowed to process sensitive personal data relating to the political, philosophical, religious or trade union objects concerning the members of that body or entity, or any other person who the body or entity regularly exchanges information with. Such processing by an entity or body is allowed if it is done in the course of its legitimate activities and with appropriate guarantees. It should also be noted that this sensitive personal data may be provided to a third party only where the data subject has given written consent.

Furthermore, processing of sensitive personal data for health or medical purposes is allowed where the processing is done by a health professional and is necessary for preventative medicine as well as protection of public health, medical diagnosis, health care or the management of health and hospital care services.

Processing sensitive personal data is also allowed where it is for research, scientific and statistics purposes so long as the processing is compatible with specified, explicitly stated and legitimate purposes. In the case of research and scientific purposes, the Commissioner must have approved the processing on the advice of a committee responsible for research and scientific ethics, whilst in the case of statistics, the processing must be necessary for the purposes provided under the Statistics Act (Cap 17:01).

There is a general prohibition against processing genetic and biometric data for what it reveals or contains. The prohibition does not apply where such data is processed in accordance with the general requirements for processing sensitive personal data as outlined above. Where genetic and biometric data is processed for medicinal purposes and the consent of the data subject has been granted, the processing must only be effected where a unique patient identification number is given to the data subject. This patient number must be different from any other identification number possessed by the data subject.

Sensitive personal data may also be processed for legal purposes where it is necessary in connection with any legal proceedings including prospective proceedings, for the purposes of obtaining legal advice, for establishing, exercising or defending legal rights, or for the administration of justice.

With respect to a data subject’s identity card number, processing in the absence of the data subject’s consent is only allowed where the processing is clearly justifiable having regard to the purpose of the processing, the importance of a secure identification or any valid reason as may be prescribed.

During the processing operation where personal data is obtained directly from the data subject, the data controllers and data processors are required to furnish to the data subject with the following information, except where the data subject already has the information:

- The identity and habitual residence or principal place of business;
- The purpose of the processing;
- The existence of the right to object to the intended processing if the processing is for purposes of direct marketing;
- Any other additional information if it will ensure fair processing, which may include the recipient or category of recipients, whether the reply to any question posed is obligatory or voluntary and the possible consequences of failure to reply as well as the existence of the right to access, rectify, delete the data concerning the data subject; or
- Any other information necessary for the specific nature of the processing, to guarantee fair processing in respect of the data subject.

A person who has access to personal data and is acting under the authorisation of the data controller or the data processor must process personal data only as instructed and without prejudice to any duty or restriction imposed by law. A contravention of this amounts to an offence which is punishable by a fine not exceeding BWP 20,000 or to imprisonment for a term not exceeding one year, or to both.

Where personal data is processed without the required authorisation, such processing amounts to an offence which is punishable by a fine not exceeding BWP 100, 000 or to imprisonment for a term not exceeding three years, or to both.

It is mandatory to safeguard the security of personal data by taking appropriate technical and organisational security measures necessary to protect the personal data from negligent or unauthorised destruction, negligent loss or the alteration, unauthorised access and any other unauthorised processing of personal data.

When taking appropriate technical and organisational security measures necessary to protect the personal data, the person doing so must ensure an appropriate level of security by taking into account:

- technological developments of processing personal data, and the costs for implementing the security measures; and
- the nature of the personal data to be protected and the potential risks involved.

Additionally, when outsourcing processing of personal data, the data processor to be chosen must be one who gives sufficient guarantees regarding the technical and organisational security measures in place for the processing to be done. The data controller or processer who outsources must ensure that the said measures are complied with.

TRANSFER

The transfer of personal data from Botswana to another country is prohibited save for transborder transfers to countries that have been designated by the Minister through an Order published in the Government Gazette.

Transborder transfers of personal data require prior authorisation to be granted by the Commissioner so as to assess and ensure that adequate levels of protection are provided by the country receiving the personal data. The assessment is in light of all the circumstances surrounding the data transfer operation and particular consideration is given to:

- the nature of the data;
- the purpose and duration of the proposed processing operation;
- the country of origin and the country of final destination;
- the rule of law, both general and sectoral, in force in the third country in question; and
- the professional rules and security safeguards which are complied with in that country.

Notwithstanding the above, transborder transfers to countries which do not offer an adequate level of protection are allowed where the data subject consents to the proposed transfer or, where the transfer is:

- necessary for the performance of a contract between the data subject and the data controller, or the implementation of pre contractual measures taken in response to the data subject’s request;
- necessary for the performance or conclusion of a contract in the interests of the data subject between the data controller and a third party;
- necessary or legally required for the public interest, or for the establishment, exercise or defence of a legal claim;
- necessary to protect the vital interests of the data subject; or
- made from a register that is intended to provide the public with information and is open to public inspection.

Regardless of the above mentioned restrictions, transborder flow of personal data to a country without adequate levels of protection may be authorised where consent is obtained from the data subject and the data controller provides adequate safeguards which may be by means of appropriate contractual provisions, with respect to the protection of the privacy and fundamental rights and freedoms of individuals.

Currently, personal data may be freely transferred to the following countries:

1. Austria
2. Belgium
3. Bulgaria
4. Croatia
5. Cyprus
6. Czech Republic

7. Denmark
8. Estonia
9. Finland
10. France
11. Germany
12. Greece
13. Hungary
14. Ireland
15. Italy
16. Latvia
17. Lithuania
18. Luxembourg
19. Malta
20. Netherlands
21. Poland
22. Portugal
23. Romania
24. Slovakia
25. Spain
26. Slovenia
27. Sweden
28. Norway
29. Liechtenstein
30. Iceland
31. The United Kingdom
32. New Zealand
33. Israel
34. Japan
35. Isle of Man
36. Guernsey
37. Switzerland
38. Uruguay
39. Republic of Korea
40. Andorra
41. Argentina
42. Foroe Islands
43. Jersey
44. South Africa
45. Kenya

SECURITY

Data controllers are required to take appropriate technical and organisational security measures necessary to protect personal data from negligent or unauthorised destruction, negligent loss, as well as unauthorised access, alteration and processing of personal data.

The measures are influenced by technological developments of processing personal data and the costs for implementing the security measures, as well as the nature of the personal data and the potential risks involved.

Failure to implement the security safeguards amounts to an offence and will render the data controller liable to a fine not exceeding BWP 500 000 or to imprisonment for a term not exceeding nine years, or to both.

BREACH NOTIFICATION

Data controllers and data processors are required to immediately notify the Commissioner of any breach to the security safeguards of personal data. A failure to do so amounts to an offence punishable by a fine not exceeding BWP 100 000 or to imprisonment for a term not exceeding three years, or to both.

ENFORCEMENT

As mentioned earlier, the Commission is the competent authority that is tasked with protection of personal data through effective application and compliance with the DPA.

ELECTRONIC MARKETING

Marketing by means of electronic communication is governed by the Electronic Communications and Transactions Act – Act No 14 of 2014 (“**ECTA**”).

An originator, who carries out marketing by means of electronic communication must provide the addressee with the originators’ identity and contact details including the place of business, e-mail, addresses and telefax number, as well as a valid and operational opt-out facility from receiving similar communications in future, and additionally, the identifying particulars of the source from which the originator obtained the addressee’s personal information.

In terms of the ECTA, unsolicited commercial communication must only be sent where the opt in requirement has been met and this includes:

- the addressee’s email address and other personal information was collected by the originator of the message in the course of a sale or negotiations for a sale;
- the marketing relates to similar products or services;
- when the personal information and address was collected by the originator, the originator offered the addressee the opportunity to opt-out, free of charge except for the cost of transmission, and the addressee declined to opt- out; and
- the opportunity to opt-out is provided with every subsequent message.

Failure to provide the addressee with an optional opt-out facility is an offence which is punishable by a fine not exceeding BWP 10 000, or to imprisonment for a term not exceeding five years, or to both. Furthermore, an originator who persists in sending unsolicited commercial communications to an addressee who has opted-out from receiving such through the originator’s opt out facility commits an offence and is liable to a fine not exceeding BWP 50 000, or to imprisonment for a term not exceeding eight years, or to both.

Also noteworthy is the DPA requirement that where personal data is processed for direct marketing purposes, the data controller must, at no cost, inform the data subject of the right to oppose the processing. Processing for such purposes will be prohibited where the data subject has given a notice of objection to the processing of the personal data. A data controller who processes the data despite the objection made by the data subject, commits an offence which is punishable by fine not exceeding BWP 500 000 or to imprisonment for a term not exceeding nine years, or to both.

ONLINE PRIVACY

There is currently no specific online privacy legislation and no provision in the DPA and the ECTA regarding such.

KEY CONTACTS

Minchin & Kelly (Botswana)

Isaac Ntombela
Partner
Minchin & Kelly (Botswana)
T +267 391 2734

intombela@minchinkelly.bw

Namie Modiri
Associate
Minchin & Kelly (Botswana)
T +267 391 2734
nmodiri@minchinkelly.bw

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BRAZIL

Last modified 28 January 2024

LAW

After several discussions and postponements, the Brazilian General Data Protection Law (LGPD), Federal Law no. 13,709/2018, entered into force on September 18, 2020. The LGPD is Brazil’s first comprehensive data protection regulation, and it broadly aligns with the EU General Data Protection Act (GDPR).

Although the law has been in force since 2020, the penalties issued by the LGPD only became enforceable on August 1, 2021. However, public authorities (such as consumer protection bodies and public prosecutors) and data subjects could enforce their rights under the LGPD as of September 18, 2020.

Before the enactment of the LGPD, data privacy regulations in Brazil consisted of various provisions spread across Brazilian legislation. For example, Federal Law no. 12,965/2014 and its regulating Decree no. 8,771/16 (together, the Brazilian Internet Act) imposed requirements regarding security and the processing of personal data and other obligations on service providers, networks, and applications providers, and provided rights for Internet users.

The following laws also contain general provisions and principles applicable to data protection:

- The Federal Constitution
- The Brazilian Civil Code, and
- Laws and regulations that address
    - Certain types of relationships (*g*., Consumer Protection Code [1] and employment laws);
    - Regulated sectors (*g*., financial institutions, health industry, or telecommunications); and
    - Particular professional activities (*g*., medicine and law).

Additionally, there are laws that regulate the processing and safeguarding of documents and information handled by governmental entities and public bodies.

The LGPD applies to any processing operation carried out by a natural person or a legal entity (of public or private law), irrespective of (1) the means used for the processing, (2) the country in which its headquarter is located, or (3) the country where the data are located, provided that:

- The processing operation is carried out in Brazil;
- The purpose of the processing activity is to offer or provide goods or services, or the processing of data of individuals located in Brazil; or
- The personal data was collected in Brazil.

On the other hand, the law does not apply to the processing of personal data that is:

- Carried out by a natural person exclusively for private and non-economic purposes;
- Performed for journalistic, artistic, or academic purposes;

- Carried out for purposes of public safety, national security, and defense or activities of investigation and prosecution of criminal offenses (which will be the subject of a specific law);
- Originated outside the Brazilian territory and are not the object of communication; or
- Shared data use with Brazilian processing agents or the object of international transfer of data with another country that is not the country of origin, provided that the country of origin offers a level of personal data protection adequate to that established in the Brazilian law.

In addition, on October 20, 2021, the Brazilian Senate unanimously approved the Proposed Amendment to the Constitution (“PEC”) no. 17/2019, which includes in the Federal Constitution the protection of personal data, including in digital media, as a fundamental right, and to refer privately to the Union (federal government) the responsibility to legislate on this subject. As of February 10, 2022, data protection is now encompassed by the Federal Constitution as a fundamental right.

---

1. Due to a broad interpretation established in case law, practically every Internet user is considered a 'consumer' for the purposes of the consumer protection.

DEFINITIONS

Definition of personal data

The LGPD defines **personal data** as any information related to an identified or identifiable natural person.

Anonymized data is not considered personal data, except when the process of anonymization has been reversed or if it can be reversed applying reasonable efforts.

Definition of sensitive personal data

The LGPD defines **sensitive personal data** as any personal data concerning:

- Racial or ethnic origin
- Religious belief
- Political opinion
- Trade union
- Religious, philosophical or political organization membership
- Health or sex life
- Genetic or biometric data

NATIONAL DATA PROTECTION AUTHORITY

The LGPD established the National Data Protection Authority (ANPD). On October 25, 2022, Law 14,460/2022 was published, altering ANPD’s role into a special and independent autarchic regime with administrative and budgetary autonomy as opposed to linking the ANPD to the Presidency of the Republic. The ANPD is also given technical and decision-making autonomy with jurisdiction over the Brazilian territory. In addition, the ANPD will have its own appointed public attorneys, which enables the National Authority to independently take judicial measures that it deems appropriate.

The ANPD is now in operation and it is headquartered in the Federal District. Its structuring process started on August 27, 2020, with the publication of Decree No. 10,474/2020, which approved and regulated the regulatory structure of the ANPD, and its board of commissioned positions and nominated trust functions. On November 6, 2020, this Decree entered into force with the appointment of the Director-President and the members of the Board of Directors of the ANPD, after having been approved by the plenary of the Federal Senate. On March 9, 2021, the ANPD’s Internal Regulations were published, establishing the competencies and organization of the National Authority.

The ANPD is composed of:

- A Board of Directors
- A national council for Personal Data and Privacy Protection (Council)
- Bodies of direct and immediate assistance to the Board of Directors (General Secretariat, General Coordination of Administration, General Coordination of Institutional and International Relations)
- An Internal Affairs Office (inspection body)
- An ombudsman
- The Prosecution
- Its own legal advisory body, and
- Administrative and specialized units for the enforcement of the LGPD (*ie*, General Coordination of Standardization; General Coordination of Supervision; and General Coordination of Technology and Research)

The ANPD has the authority to issue sanctions for violations of the LGPD. This sanctions authority came into force on August 1, 2021. On October 29, 2021, the ANPD issued Regulation CD/ANPD 01/2021 for the Regulation of the Inspection Process and the Sanctioning Administrative Process, establishing the procedures regarding the supervision and enforcement of the LGPD. However, the Regulation is still pending further instructions relating to the parameters of calculation of such penalties, which are expected to be regulated by the end of 2023.

In August 2021, the President of the Republic appointed representatives of the National Council for Personal Data and Privacy Protection (Council). The Council contributes to the performance of the ANPD and has the authority to, among other things:

- Oversee the protection of personal data
- Issue regulations and procedures related to personal data protection
- Deliberate, at an administrative level, upon the interpretation of the LGPD and matters omitted in its redaction
- Supervise and apply sanctions in the event of data processing performed in violation of the legislation
- Implement simplified mechanisms for recording complaints about the processing of personal data in violation of the LGPD

In addition, the ANPD Council is responsible for, among other functions:

- Proposing strategic guidelines and allowance for the creation of the National Policy for the Protection of Personal Data and the operation of ANPD
- Suggesting actions to be carried out by the ANPD
- Preparing studies and conducting public debates and hearings about the protection of personal data

Since the ANPD started its operations, several actions have already been implemented to protect personal data, including:

- Determining the procedures regarding the inspection and application of administrative sanctions
- Providing specific regulation regarding small-sized data processing agents
- Publishing guidelines regarding cookie policy and banner
- Opening public consultation regarding international transfers
- Publishing guidance on reporting a security incident with personal data and its assessment to the ANPD
- Explaining availability of a claim by the data subject against controller
- Providing educational materials on data protection, such as (1) guidelines for defining personal data processing agents and the DPO, (2) how consumers should protect their personal data, and (3) information security for small processing agents.

However, there are still several provisions of the LGPD requiring further regulation and interpretation by the ANPD, which stakeholders should monitor for future compliance.

REGISTRATION

There is currently no requirement to register with the National Data Protection Authority under Brazilian law.

DATA PROTECTION OFFICERS

The LGPD creates the position of Chief of Data Processing, which is the data protection officer (DPO) in charge of data processing operations. The DPO is responsible for the following:

- Accepting complaints and communications from data subjects and the National Authority
- Providing guidance to employees about good practices and carrying out other duties as determined by the controller or set forth in complementary rules

The LGPD provides the National Data Protection Authority the power to further establish supplementary rules concerning the definition and the duties of the DPO, including scenarios in which the appointment of such person may be waived, according to the nature and the size of the entity or the volume of data processing operations.

Currently, with the exception mentioned below, every company, public or private, should appoint a DPO. This general obligation extends to all types of activities and volumes of data processing subject to the LGPD (as set out in the “Guidance on Processing Agents and DPO” published by ANPD in May 2021). In any case, all companies should monitor this space for future guidance. On December 23, 2022, the ANPD published updated breach guidelines, which require companies to provide the DPO’s nomination declaration as a necessary document to report any breaches. Therefore, although is not expressly required by the LGPD, it must practically be considered as essential and necessary documentation.

On August 30, 2021, the ANPD issued a Public Consultation related to a Resolution with special rules on the application of the LGPD to small businesses, startups, and innovative companies, as defined by the law, except for those performing data processing activities which incur in high risks for data subjects.[1] As a result, on January 28, 2022, the ANPD published Regulation CD/ANPD 02/2022, which establishes simpler obligations for small businesses, including an exception to nominate a DPO.

There is no prohibition against companies using an external DPO or against DPOs performing the same function for more than one company simultaneously. Likewise, the LGPD does not distinguish whether the DPO must be an individual or a legal entity.

Due to the absence of legal or regulatory requirements, there is no need to communicate or record the identity and contact information of the DPO with the ANPD.

FN 1:

The following entities are considered Small-Sized Processing Agents:

- micro-enterprises and small size businesses, as defined by Art. 41, Law No 14,195/2021
- entrepreneur, as defined by the Civil Code No 10,406/2002
- start-ups, as defined by Law No 182/2021
- non-profits organizations
- natural persons and depersonalized private entities who carry out treatment of personal data, assuming typical controller or operator obligations.

Small-Sized Processing Agents must not earn gross revenue higher than BRL 4.800.000,00, or, in the case of start-ups BRL 16.000.000,00, nor belong to an economic group whose global revenue exceeds the limits, as defined by the corresponding laws or perform high-risk processing. According to the Regulation, a high-risk data processing activity meets at least one general and one specific criteria among those listed in the Regulation. General criteria are: (i) processing of personal data in large scale; and (ii) processing of personal data which may significantly affect the data subjects’ interests and fundamental rights, while specific criteria is (i) use of emerging or innovative technologies; (ii) vigilance or control of public accessible areas; (iii) decisions made exclusively with basis on automated data processing; and (iv) use of sensitive data or personal data belonging to children, adolescents and elderly people.

COLLECTION & PROCESSING

Under the LGPD, collecting and processing are referred to as "data treatment", and defined as all operations carried out with personal data, such as:

- Collection
- Production

- Reception
- Classification
- Utilization
- Access
- Reproduction
- Transmission
- Distribution
- Processing
- Filing
- Storage
- Elimination
- Evaluation
- Control
- Modification
- Communication
- Transfer
- Diffusion, or
- Extraction

The processing of personal data may only be carried out based on one of the following legal bases:

- With data subject consent
- To comply with a legal or regulatory obligation by the controller
- By the public administration, for the processing and shared use of data which are necessary for the execution of public policies provided in laws or regulations or contracts, agreements or similar instruments
- For carrying out studies by research entities, ensuring, whenever possible, the anonymization of personal data
- For the execution of a contract or preliminary procedures related to a contract to which the data subject is a party
- For the regular exercise of rights in judicial, administrative or arbitration procedures
- As necessary for the protection of life or physical safety of the data subject or a third party
- For the protection of health, exclusively, in a procedure carried out by health professionals, health services or sanitary authorities
- To fulfill the legitimate interests of the controller or a third party, except in the case of prevailing the fundamental rights and freedoms of the data subject, and
- For the protection of credit

Notwithstanding the above, personal data processing must be carried out in good faith and based on the following principles:

- Purpose
- Suitability
- Necessity
- Free access
- Quality of the data
- Transparency
- Security
- Prevention
- Nondiscrimination, and
- Accountability

As for the processing of sensitive personal data, the processing can only occur when the data subject or their legal representative consents specifically and in highlight, for specific purposes; or, without consent, under the following situations:

- As necessary for the controller’s compliance with a legal or regulatory obligation
- Shared data processed as necessary for the execution of public policies provided in laws or regulations by the public administration

- For carrying out studies by research entities, ensuring, whenever possible, the anonymization of personal data
- For the regular exercise of rights, including in a contract or in a judicial, administrative or arbitration procedure
- Where necessary for the protection of life or physical safety of the data subject or a third party
- The protection of health, exclusively, in a procedure performed by health professionals, health services or sanitary authorities, or
- To prevent fraud and protect the safety of the data subject

The controller and operator must keep records of the data processing operations they carry out, mainly when the processing is based on a legitimate interest.

In this sense, the ANPD may determine that the controller must prepare an Impact Report on Protection of Personal Data, including sensitive data, referring to its data processing operations, pursuant to regulations, subject to commercial and industrial secrecy. The report must contain at least a description of the types of data collected, the methodology used for collection and for ensuring the security of the information, and the analysis of the controller regarding the adopted measures, safeguards and mechanisms of risk mitigation.

On January 28, 2022, the ANPD published Regulation CD/ANPD 02/2022, which provides special rules on the application of the LGPD to small businesses, startups, and innovative companies, as defined by the law, except to those performing data processing activities which incur in high risks for data subjects.[1] This Regulation includes certain exemptions and flexibilities, reducing obligations under the law. For example a simplified template of records of data processing activities, which will be made available by the ANPD.

FN 1:

The following entities are considered Small-Sized Processing Agents:

- micro-enterprises and small size businesses, as defined by Art. 41, Law No 14,195/2021
- entrepreneur, as defined by the Civil Code No 10,406/2002
- start-ups, as defined by Law No 182/2021
- non-profits organizations
- natural persons and depersonalized private entities who carry out treatment of personal data, assuming typical controller or operator obligations.

Small-Sized Processing Agents must not earn gross revenue higher than BRL 4.800.000,00, or, in the case of start-ups BRL 16.000.000,00, nor belong to an economic group whose global revenue exceeds the limits, as defined by the corresponding laws or perform high-risk processing. According to the Regulation, a high-risk data processing activity meets at least one general and one specific criteria among those listed in the Regulation. A general criteria is (i) processing of personal data in large scale; and (ii) processing of personal data which may significantly affect the data subjects’ interests and fundamental rights, while specific criteria is (i) use of emerging or innovative technologies; (ii) vigilance or control of public accessible areas; (iii) decisions made exclusively with basis on automated data processing; and (iv) use of sensitive data or personal data belonging to children, adolescents and elderly people.

TRANSFER

The transfer of personal data to other jurisdictions is allowed only subject to compliance with the requirements of the LGPD. Prior specific and informed consent is needed for such transfer, unless:

- The transfer is to countries or international organizations with an adequate level of protection of personal data
- There are adequate guarantees of compliance with the principles and rights of data subject provided by LGPD, in the form of
    - Specific contractual clauses for a given transfer
    - Standard contractual clauses
    - Global corporate norms, or

    - Regularly issued stamps, certificates and codes of conduct
- The transfer is necessary for international legal cooperation between public intelligence, investigative and prosecutorial agencies
- The transfer is necessary to protect the life or physical safety of the data subject or a third party
- The ANPD has provided authorization
- The transfer is subject to a commitment undertaken through international cooperation
- The transfer is necessary for the execution of a public policy or legal attribution of public service
- The transfer is necessary for compliance with a legal or regulatory obligation, execution of a contract or preliminary procedures related to a contract, or the regular exercise of rights in judicial, administrative or arbitration procedures

On May 05, 2022, ANPD opened a public consultation regarding international transfers regulation. However, such regulation is pending but expected to be published sometime in 2023.

SECURITY

Controllers and processors must adopt technical and administrative security measures designed to protect personal data from:

- Unauthorized accesses, and
- Accidental or unlawful situations of:
    - Destruction
    - Loss
    - Alteration
    - Communication, or
    - Any improper or unlawful processing

The LGPD grants the ANPD authority to establish minimum technical standards for companies to implement.

On 4 October 2021, the ANPD launched information security guidelines aimed at small data processing agents (such as microenterprises, small businesses, and startups) to assist them with good practices in implementing technical and administrative information security measures for the protection of personal data. The guidelines also contain a checklist to facilitate the visualization of suggestions, such as awareness and training programs, agreements management, access controls, data storage guidelines, and vulnerability management.

On November 04, 2022, the ANPD published its Regulatory Agenda for 2023/2024 and made the regulation of technical and administrative security measures a priority for the period, determining the start of the regulation procedures until the beginning of 2024.

The Brazilian Internet Act further establishes that service providers, networks and applications providers should keep access records (such as IP addresses and logins) confidential and in a secured and controlled environment. Guidelines issued under the Internet Act established guidelines on appropriate security controls, including:

- Strict control on data access by defining the liability of persons who will have the possibility of access and exclusive access privileges to certain users
- Prospective of authentication mechanisms for records access, using, for example, dual authentication systems to ensure individualization of the controller records
- Creation of detailed inventory of access to connection records and access to applications containing the time, duration, the identity of the employee or the responsible person for the access designated by the company and the accessed file
- Use of records management techniques that ensure the inviolability of data, such as encryption or equivalent protective measures

BREACH NOTIFICATION

According to the LGPD, any unauthorized accesses and from accidental or unlawful situations of destruction, loss, alteration, communication or diffusion is considered a breach. The controller is responsible for reporting to ANPD and the data subject within a reasonable timeframe if the breach is likely to result in risk or harm to data subjects. The LGPD itself does not set a

specific deadline for notifying the ANPD in the event of security incidents. However, according to guidance published by the National Authority on February 22, 2021, the communication must be made within two (2) working days, counted from the date of receiving knowledge of the incident.

In addition, according to these guidelines, the company or person responsible for the data must internally assess the incident and ascertain the nature, category, and number of data subjects affected.

On December 23, 2022, the ANPD published updated breach guidelines, which include additional recommendations (as further specified below) as well as an updated breach reporting form, which must be used for regulator notification if notification is required under the law. In the event of significant risk or damage to data subjects, individuals may need to be notified as well. Notification may be submitted by the Controller’s DPO or the legal representative, with the corresponding nomination documentation or power of attorney.

The notice must contain, at least, the following key information:

- Description of the nature of the affected personal data
- Information regarding the data subjects involved
- Indication of the security measures used
- The risks generated by the incident
- The reasons for a delay in communication (if any)
- The measures that were or will be adopted
- Information regarding the communication to the affected data subjects

Additionally, the ANPD must verify the seriousness of the incident and may, if necessary to safeguard the data subject's rights, order the controller to adopt measures, such as the broad disclosure of the event in communications media, as well as measures to reverse or mitigate the effects of the incident.

The updated guidelines indicate that an unjustified delay in reporting a security incident that could cause significant risk or damage to data subjects may subject agents to the administrative sanctions provided under the LGPD. In case the Controller is unable to provide a complete breach notification within the two (2) working days period, the Controller must submit a preliminary notice with the corresponding justification. The preliminary notice must be supplemented as soon as possible and, at the latest, within 30 calendar days.

Although it is not necessary to provide the list of affected data subjects to the ANPD, the ANPD may request the Controller, at any time, to present a copy of the notice to the data subjects regarding the breach. Such notice to the data subject must be made individually, whenever possible, and can be carried out by any means, such as e-mail, letter or electronic message.

An additional recommendation, which is not legally required, is to implement contractual clauses establishing the obligations regarding notification of breaches between controllers and processors, seeking to expedite the assessment and minimize the risks to the data subjects.

On January 28, 2022, the ANPD published Regulation CD/ANPD 02/2022 which grants to small businesses, startups, and innovative companies, as defined by the law, except to those performing data processing activities which incur in high risks for data subjects the double deadline extension in the communication of security incidents, as well responding to data subjects’ requests, for communicating severe security incidents to the ANPD and affected data subjects, and for responding to ANPD’s requests.

ENFORCEMENT

The LGPD provides for penalties in case of violations its provisions. Data processing agents that commit infractions can be subject to administrative sanctions, in a gradual, single or cumulative manner, including a fine, simple or daily, of up to 2% of the revenues of a private legal entity, group or conglomerate in Brazil, up to a total maximum of R$50 million per infraction.

Other sanctions can include:

- Warning

- Publicizing of the violation
- Blocking the personal data to which the infraction refers to until its regularization
- Deletion of the personal data to which the infraction refers
- Partial suspension of the database operation to which the infringement refers for a maximum period of six (6) months, extendable for the same period, until the processing activity is corrected by the controller;
- Suspension of the personal data processing activity to which the infringement refers for a maximum period of six (6) months, extendable for the same period;
- Partial or total prohibition of activities related to data processing.

Although the LGPD became effective September 18, 2020, the penalties provided by the law were only enforceable from August 1, 2021. In addition, the ANPD is now in operation and, on October 29, 2021, published the Regulation of the Inspection Process and the Sanctioning Administrative Process, which establishes the procedures applicable to ANPD’s inspection process and the rules to be observed during the administrative sanctioning process. However, it is still pending further instructions relating to the parameters of calculation of such penalties, which are expected to be regulated until the end of 2023. Because the ANPD has not imposed sanctions regarding violations to the LGPD yet, the level of enforcement activity is still uncertain.

Public authorities (such as consumer protection bodies and public prosecutors) are already monitoring data protection matters and applying penalties based on the LGPD obligations and other applicable laws. Additionally, data subjects may file lawsuits if any of the rights provided by the LGPD are violated. Under the law, a controller or processor that causes material, moral, individual, or collective damage to others is liable to individuals for such damages, including through a class action.

Exceptions to the obligation to remedy a violation exist only if:

- The agent (*ie*, controller or the processor) did not carry out the data processing
- There was no violation of the data protection legislation in the processing, or
- The damage arises due to exclusive fault of the data subject or a third party

ELECTRONIC MARKETING

Brazil has no specific law regulating electronic marketing communications. However, it is important to point out that, according to the LGPD, all processing of consumers’ personal data (which includes the collection, storage, and sending of marketing communications) can only occur upon the appropriate legal basis for such purpose. Under this scenario, two available legal bases could be used, depending on the analysis of the concrete case: (1) the data subject’s consent, or (2) the controller’s legitimate interest.

Despite the lack of a specific statute, general provisions on privacy and intimacy rights, as well as consumer protection rights, also apply to electronic marketing. Therefore, the sender should immediately cease sending any electronic marketing if the consumer requests (i.e., offering an opt-out option to electronic marketing).

ONLINE PRIVACY

The Brazilian Internet Act has several provisions concerning the storage, use, disclosure, and other processing of data collected on the Internet. The established rights of privacy, intimacy, and consumer rights apply equally to electronic media, such as mobile devices and the Internet. Violations of these rights may also be subject to civil enforcement.

Furthermore, as explained in prior sections, identifiable data are also encompassed under the scope of protection of the LGPD. Thus, if cookies and location data are associated with a natural person, their collection should also observe the same obligations provided by the Brazilian data protection law. However, the obligation does not apply to anonymized data, which is not considered personal data under the LGPD unless the process of anonymization has been reversed or can be reversed using reasonable efforts.

That said, a proper legal basis is needed when using cookies and similar technologies that involve the processing of a user’s personal data from (e.g., the information is linked or linkable to a particular user, IP address, a device, or other particular identifier). Under this scenario, two available legal bases could be used, depending on the analysis of the concrete case: the data subject’s consent or the controller’s legitimate interest (in the case of essential cookies, for example).

On October, 2022, the ANPD published Cookie Guidelines establishing recommendations for cookie policy disclosures, such as to inform the categories of relevant cookies, their purposes, retention periods and whether the data collected through cookies is shared. Such disclosures must be provided to the data subject in a simplified and understandable format and manner. Further, the guidelines require collection of affirmative opt-in consent, for example through cookie banners, and provide the data subject with the possibility to reject the cookies at that time and revoke consent at any time later on.

KEY CONTACTS

Campos Mello Advogados
www.camposmello.adv.br/

Paula Mena Barreto
Partner
Campos Mello Advogados
T +55 21 3262 3028
paula.menabarreto@cmalaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BRITISH VIRGIN ISLANDS

Last modified 28 January 2024

LAW

The British Virgin Islands' Data Protection Act, 2021 (DPA) came into force on 9 July 2021.

The DPA is the primary legislation and the first legislative framework of its kind in the British Virgin Islands to govern how public and private bodies may process personal data. The law strives to promote transparency and accountability, bringing the British Virgin Islands in line with the UK and EU data protection standards.

DEFINITIONS

Definition of personal data

Personal data means any information in respect of commercial transactions which: (i) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (ii) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (iii) is recorded as part of a relevant filing system or with the intention, and in each case, that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information, or from that or other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject

Definition of sensitive personal data

Sensitive personal data means any personal data about a data subject’s:

- physical or mental health;
- sexual orientation;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- criminal convictions, the commission or alleged commission of, an offence; or
- any other personal data that may be prescribed as such under the DPA, from time to time.

Other key definitions

commercial transactions means any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking, and insurance

data processor, in relation to personal data, means a person who processes data on behalf of a data controller but does not include an employee of the data controller

data subject means a natural person, whether living or deceased

data controller means a person who, either alone or jointly, or in common with other persons, processes any personal data, or has control over, or authorises the processing of any personal data, but does not include a data processor

processing, in relation to personal data, means collecting, recording, holding, or storing the personal data or carrying out any operation or set of operations on the personal data, including the: (i) organisation, adaptation, or alteration of personal data; (ii) retrieval, consultation or use of personal data; (iii) disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or (iv) alignment, combination, correction, erasure or destruction of personal data, and

NATIONAL DATA PROTECTION AUTHORITY

The supervisory authority under the DPA is the Office of the Information Commissioner.

Given the recent enactment of the DPA, the Office of the Information Commissioner has not yet been staffed.

REGISTRATION

There is currently no requirement for a data controller or a data processor to notify the Information Commissioner of their role or complete any registration.

DATA PROTECTION OFFICERS

There is no requirement under the DPA for a data protection officer to be appointed.

COLLECTION & PROCESSING

Data controllers are responsible for compliance with certain privacy and data protection principles applicable to the personal data it processes. Data controllers are also responsible for ensuring that the principles are complied with, where personal data is processed on the data controller’s behalf (e.g., by its vendors).

Under these principles:

- a data controller shall not process personal data (other than sensitive personal data) without the express consent of the data subject, or transfer personal data outside of the British Virgin Islands without proof of adequate data protection safeguards or consent from the data subject, unless either of the Exceptions defined under the heading “ Transfer” exists (the **General Principle**)
- a data controller must inform a data subject of: (a) the purposes for processing; (b) information as to the source of the personal data; (c) the rights to request access to and correction of the personal data; (d) how to contact the data controller; (e) the class of third parties to whom the personal data will be disclosed; and (f) whether the data is obligated to supply the personal data, and if so, the consequences of not supplying same (the **Notice and Choice Principle**)
- no personal data shall be disclosed without the consent of the data subject for any purposes other than the purpose for which the personal data was to be disclosed at the time of collection or to any party other than a third party of the class of third parties noted above (the **Disclosure Principle**)
- a data controller must take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration, or destruction by having regard to (a) the nature of the personal data and the harm that would result from any loss, misuse, etc.; (b) the place or location where the personal data is stored; (c) any security measures incorporated into any storage equipment; (d) the measures taken for ensuring the reliability, integrity, and competence of personnel having access to the personal data; and (e) the measures taken for ensuring the secure transfer of the personal data (the **Security Principle**)
- personal data shall not be kept longer than is necessary for the fulfillment of the purpose of processing, and data controllers must take all reasonable steps to ensure that personal data is destroyed or permanently deleted if no longer required for the purpose for which it was to be processed (the **Retention Principle**)
- a data controller shall take reasonable steps to ensure that personal data is accurate, complete, not misleading, and kept current (the **Data Integrity Principle**), and
- data subjects shall be given access to their personal data and be able to request corrections where the personal data is inaccurate, incomplete, misleading, or not current (the “**Access Principle**”)

TRANSFER

As set out under the **General Principle**, transfers of personal data by a data controller or a data processor to countries or territories outside the British Virgin Islands are only permitted where that country or territory ensures an adequate level of protection of data protection safeguards in relation to the processing of personal data. This transfer restriction endeavors to ensure that the level of protection provided by the DPA is not circumvented by transferring personal data abroad.

The DPA also includes the following exceptions where the General Principle will not apply to a transfer:

- if the data subject has consented to the transfer (where consent must be freely given, specific, informed, and unambiguous and must be capable of being withdrawn at any time)
- where the transfer is necessary for the performance of a contract between the data subject and the data controller, or the taking of steps at the request of the data subject with a view to the data subject entering into a contract with the data controller
- the transfer is necessary for the conclusion of a contract between the data controller and a person other than the data subject, being a contract that is entered into at the request of the data subject, or is in the interests of the data subject, or for the performance of such a contract;
- the transfer is necessary for reasons of substantial public interest
- the transfer is for a lawful purpose directly related to an activity of the data controller, is necessary for, or directly related to, that purpose, and the personal data is adequate but not excessive in relation to that purchase
- the transfer is necessary in order to protect the vital interests of the data subject
- the transfer is necessary for the administration of justice, or
- the transfer is required for the exercise of any functions conferred on a person by law.

SECURITY

While the DPA does not specify any technical standards for data controllers to implement, the DPA requires a data controller, when processing personal data, to take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access, or disclosure, alteration or destruction (together, '**Security Breach**') by having regard to the following matters:

- the nature of the personal data and the harm that would result from a Security Breach
- the place or location where the personal data is stored
- any security measures incorporated into any equipment in which the personal data is stored
- the measures taken for ensuring the reliability, integrity, and competence of personnel having access to the personal data, and
- the measures taken for ensuring the secure transfer of the personal data

The DPA also requires, where a data processor carries out the processing of personal data on behalf of the data controller, the data controller (for the purpose of protecting the personal data from Security Breach) to ensure that the data processor:

- provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and
- take reasonable steps to ensure compliance with the above measures

BREACH NOTIFICATION

The DPA does not require data controllers to notify the Information Commissioner or the data subjects of personal data breaches.

However, notice requirements apply to data controllers that receive enforcement notices from the Information Commissioner. The DPA requires a public or private body to, as soon as practicable, and in any event within 30 days of complying with an

enforcement notice from the Information Commissioner: (i) notify the data subject(s) concerned; and (ii) any person to whom the personal data was disclosed within the twelve months preceding the date of service of the enforcement notice (as determined by the Information Commissioner).

ENFORCEMENT

A breach of the DPA constitutes a criminal offence. Upon conviction, violators may be subject to a fine of up to US$100,000, imprisonment of up to five years, or both. A body corporate is punishable on conviction to a fine of up to US$500,000.

The Information Commissioner has broad investigative and corrective powers under the DPA, including the power to request and obtain information from parties subject to the law and to issue orders to carry out specific remediation activities.

The DPA provides for a private right of action where data subjects suffer damage or distress due to a breach of the DPA by a public or private body.

In addition, the DPA explicitly provides for personal liability in respect of offences committed by a body corporate where the offence is proven to have been committed with the consent or connivance of, or to be attributable to neglect on the part of, any director, secretary, or similar officer, or any person purporting to act in such capacity. Where the affairs of a body corporate are managed by its members, this personal liability also applies to the acts and defaults of a member in connection with the member’s function of management.

ELECTRONIC MARKETING

The DPA applies to “direct marketing”, which is the communication, by whatever means, of any advertising or marketing material that is directed to particular individuals and therefore includes electronic marketing.

Prior express consent is not required for the purposes of direct marketing. However, a data subject has an unconditional right to require the date controller to stop, or not to commence, the processing of any of their personal data for the purposes of direct marketing (i.e., an “opt-out” right).

ONLINE PRIVACY

There are no specific restrictions on online privacy in the DPA. However, the provisions of the DPA apply where a private body is a website operator that collects personal data.

KEY CONTACTS

Carey Olsen
www.careyolsen.com

Clinton Hempel
Partner
Carey Olsen
T +27 76 412 6091
clinton.hempel@careyolsen.com

Jude Hodge
Counsel
Carey Olsen
T +1 284 394 4034
jude.hodge@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BRUNEI

Last modified 3 January 2024

LAW

At present there are no statutory or common law obligations that protects the privacy of information upon which an individual can be directly or indirectly identified, save in respect of banker – customer relationship where banks are under a legal duty to keep customer information confidential.

However, with the publication of the Public Consultation Paper on Personal Data Protection for the Private Sector in Brunei Darussalam by the Authority for Info-communications Technology Industry of Brunei Darussalam (**AITI**) on 20 May 2021 and the Response to Feedback on Public Consultation Paper on Personal Data Protection for the Private Sector published on 3 December 2021 (together, the **Public Consultation Paper**), it is anticipated that the Personal Data Protection Order (**PDPO**) will be enacted and come into force in the near future. Premise on the Public Consultation Paper, which sets out in general terms the data protection framework under the PDPO, it is anticipated that the PDPO will introduce obligations on the part of private sector organizations with respect to collection, use, disclosure or other processing of individuals' personal data and the rights of individuals in relation to the processing of their personal data.

DEFINITIONS

Definition of personal data

At present there is no legal definition.

It is anticipated that under the PDPO "personal data" will refer to data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organization has or is likely to have access. Premised on such a definition of “personal data” it is envisaged that if a data subject cannot be identified by that data and other information to which the organization has or may have access to, such data would not come within the meaning of “personal data” under PDPO and this would remain the situation regardless of any anonymisation technique having been applied to the data. Noting that there are complexities surrounding the concept of anonymisation, AITI have expressed their intentions to provide guidance on anonymisation in due course.

Definition of sensitive personal data

At present there is no legal definition.

It is anticipated that the PDPO will not make a distinction between sensitive and non-sensitive personal data or define a category of “sensitive personal data”.

NATIONAL DATA PROTECTION AUTHORITY

At present nil.

It is anticipated that the PDPO will establish a national data protection authority referred to as the Responsible Authority. It is anticipated that AITI will be designated as the Responsible Authority.

REGISTRATION

At present no legal requirement.

It is anticipated that the PDPO will not have any registration requirements.

DATA PROTECTION OFFICERS

At present no legal requirement.

It is anticipated that the PDPO will require an organization to appoint a data protection officer who shall be responsible for ensuring that the organization complies with the PDPO and develops and implement policies and practices that are necessary to meet its obligations under the PDPO including a process to receive complaints. AITI have expressed the possibility of them issuing advisory guidelines to provide clarity and guidance on the topic of Data Protection Officers in the future.

COLLECTION & PROCESSING

At present not a regulated activity.

Under the PDPO framework set out in the Public Consultation Paper, organizations may collect, use or disclose personal data about an individual for purposes that a reasonable person would consider appropriate in the circumstance.

It is anticipated that under the PDPO organizations may collect, use or disclose personal data where:

- they have the prior consent of the individual;
- unless otherwise required or authorized by law; or
- an exception in the PDPO applies.

Where consent is required, it is anticipated that the PDPO will not specifically prescribe the manner in which consent may be given and that the PDPO will recognize that consent may be explicit or implicit through an individual’s actions or inactions, depending on the circumstances, and thereby allowing organizations flexibility as to how they obtain consent. That said, it is anticipated that the PDPO would require organizations to look to express consent as the first port of call and only rely on deemed consent or the exceptions to consent if obtaining consent is impractical or if they have otherwise failed to obtain express consent.

It is anticipated that under the PDPO consent must be validly obtained and consent would not be valid where:

- consent is obtained as a condition of providing a product or service and such consent is beyond what is reasonable to provide the product or service to the individual; the principle being that organizations should not collect more personal data than is reasonable and necessary; and
- where false or misleading information was provided in order to obtain or attempt to obtain the individual’s consent for collecting, using or disclosing his personal data.

As part of obtaining valid consent, it is anticipated that the PDPO will require organizations to provide the individual with information on:

- the purposes for the collection, use or disclosure of his personal data, on or before collecting the personal data; and
- any other purpose for the use or disclosure of personal data that has not been notified to the individual, before such use or disclosure of personal data.

Further, it is anticipated that fresh consent would be required where personal data collected is to be used for a different purpose from which the individual originally consented.

For a minor (a person below the age of 18 years) who is unable to give consent to an organisation to collect, use and disclose his personal data, the organisation will have to obtain consent from a parent or legal guardian of the minor. AITI have expressed their intentions to provide guidance on data processing activities relating to minors in the future.

TRANSFER

At present not a regulated activity.

It is anticipated that under the PDPO, an organization shall not transfer personal data to a country outside Brunei Darussalam except in accordance with requirements prescribed under the PDPO to ensure that the transferred personal data will be accorded a standard of protection that is comparable to that under the PDPO. It is not anticipated that such requirement prescribed by the PDPO will be as stringent and prescriptive as in other jurisdiction, for example the EU, and it is anticipated that the PDPO will place the onus on organizations to ensure that appropriate measures are taken to protect personal data transferred out of Brunei Darussalam through the imposition of contractual obligations or otherwise.

AITI recommends the adoption of the ASEAN Model Contractual Clauses for Cross Border Data Flows (**MCCs**) which are templates for contractual terms and conditions which may be included in legal agreements between businesses to ensure personal data is protected when engaging in cross border data transfers between ASEAN Member States. But it remains to be seen if the adoption of the MCCs will be popular as it is envisaged that a fair amount of modification will have to be made to the MCCs so as to be compatible with the purposes of any particular cross-border transaction between organisations.

SECURITY

At present not a regulated activity save in relation to a "Financial Institution" — see Mandatory Breach Notification.

It is anticipated that under the PDPO, an organization must protect personal data in its possession or under its control by making reasonable security arrangements to prevent:

- unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks; and
- the loss of any storage medium or device on which personal data is stored.

It is anticipated that under the PDPO data intermediaries will also be subjected to the same obligation to protect personal data in their possession.

It is anticipated that the PDPO will provide for a reasonable standard for such security measures taking into account factors such as the nature and sensitivity of the data, the form in which personal data is stored and the impact to the individual if the personal data is subject to unauthorized access, disclosure or other risks. But it is not anticipated that the PDPO will stipulate specific security measures to be adopted and implement by organizations and data intermediaries. That said, AITI have expressed their intentions to issue detailed guidance on the types of security measures, which will include administrative / organisational, physical and technical security measures in due course.

BREACH NOTIFICATION

Mandatory Breach Notification

At present no legal requirement save in relation to a "Financial Institution" (i.e. banks, insurance companies, moneylenders, pawnbrokers, moneychangers and securities service providers licensed in Brunei Darussalam).

It is anticipated that under the PDPO, organizations are required to, as soon as practicable, but in any case no later than 3 calendar days after the assessment, notify the Responsible Authority of a data breach that:

- results in, or is likely to result in, significant harm to the individuals to whom any personal data affected by a data breach relates; or
- is or is likely to be, of a significant scale.

AITI have expressed their intentions to issue guidelines on “significant harm” and “significant scale” in the near future.

Organizations are also anticipated to be required to notify the affected individuals on or after notifying the Responsible Authority if the data breach results in, or is likely to result in, significant harm to an affected individual.

Further, it is anticipated that unreasonable delays in reporting breaches that cannot be justified will be considered a breach of the data breach notification obligation.

Where a data breach is discovered by a data intermediary, it is anticipated that under the PDPO, the data intermediary will be under a duty to notify the organization or the Responsible Authority of the data breach.

A Financial Institution is obliged to report to the Brunei Darussalam Central Bank, no later than 2 hours after confirmation of all instances of cyber intrusion, disruption, malfunction, error or cybersecurity issues on a Financial Institution's system, server, network or end-point which has a severe or widespread impact on the operations and service delivery or has a material impact on the Financial Institution.

ENFORCEMENT

At present no enforcement authority.

It is anticipated that under the PDPO the Responsible Authority will administer and enforce the PDPO and will have the powers to do any of the following:

- issue directions to organizations to:
  - stop collecting, using or disclosing personal data in contravention of the PDPO;
  - destroy personal data collected in contravention of the PDPO; or
  - provide access to or correct personal data.
- impose a financial penalty of up to BND1 million or 10% of the annual turnover of on an organization for negligent or intentional breach of the PDPO.

ELECTRONIC MARKETING

No legal requirement to have privacy policies.

ONLINE PRIVACY

No legal requirement to have privacy policies.

KEY CONTACTS

Abraham, Davidson & CO.
www.adcobrunei.com/

Linus Tan
Partner
Abraham, Davidson & CO.
T +673 2242840
linus_tan@adcobrunei.com

Elaiza Hanum Merican
Associate
Abraham, Davidson & CO.
T +673 2242840
elaiza@adcobrunei.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BULGARIA

Last modified 21 December 2023

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

Bulgaria implemented the EU Data Protection Directive 95/46/EC with the Personal Data Protection Act (In Bulgarian: *Закон за защита на личните данн и*), promulgated in the State Gazette No. 1 of January 4, 2002, as amended periodically (Act). The Act came into force on January 1, 2002.

In view of the entry into force of Regulation (EU) 2016/679 (General Data Protection Regulation – 'GDPR'), the Personal Data Protection Act was amended by a law for amendment and supplementation which was promulgated in the State Gazette No. 17 of February 26,2019.

The Personal Data Protection Act as amended (hereinafter referred to as the 'Personal Data Protection Act) serves a twofold purpose – it effectively implements the GDPR into national legislation and also transposes Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

The Personal Data Protection Act complements the GDPR by providing regulation to matters in the field of personal data processing that have not been explicitly covered by the GDPR, or where the GDPR has left room for the exercise of legislative discretion. As the regulation has direct effect and is applicable in all EU member-states without the need of adopting a designated legislative act, the Bulgarian legislator has adopted the approach of directly referring to and implementing the GDPR without repeating the core provisions of the regulation in the Personal Data Protection Act.

Under the Personal Data Protection Act the role of supervising authority is shared between the Commission for Personal Data Protection and the Inspectorate to the Supreme Judicial Council, the latter having competence only with regards to data processing by courts, prosecution offices and criminal investigative bodies in their capacity as judicial authorities. The Personal Data Protection Act further regulates the legal remedies in cases of violation of personal data law, the accreditation and certification in the field of personal data protection, the administrative liability and the administrative measures in cases of violations of its provisions.

Pursuant to an amendment in the Personal Data Protection Act which came into force in May 2023, the Commission for Personal Data Protection was also designated as the competent controlling body under the Bulgarian Whistleblower Protection Act.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

Definition of personal data

The definition of personal data set forth before by the Personal Data Protection Act was repealed following the implementation of the GDPR and it explicitly refers to the definition of personal data under art. 4 of the GDPR (§1 of the Supplementary provisions of the Personal Data Protection Act).

Personal data means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Definition of sensitive personal data

The Personal Data Protection Act refers explicitly to the definition under the GDPR which applies following its direct effect in all EU member states.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Bulgarian data protection authority (DPA) is the Personal Data Protection Commission (In Bulgarian: *К омисия за защит а на личните дан ни*, the 'Commission').

2 Professor Tsvetan Lazarov, Sofia 1592
Bulgaria

kzld@cpdp.bg
www.cpdp.bg

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

The requirement for registration of data controllers before the Commission for Personal Data Protection was repealed with the implementation of the GDPR.

Pursuant to the Personal Data Protection Act, the Commission for Personal Data Protection maintains the following public registers:

- register of data controller and data processors who have appointed data protection officers containing the name of the data controller / data processor, the name of the appointed data protection officer and its contact details;
- register of the accredited certifying bodies under art. 14 containing information on the name and the contact details of the certifying body and on the period of validity of its accreditation;
- register of codes of conduct which includes the name of the code, the name of the editor and the relevant certification body, information about the sector concerned and its content.

The Commission shall also support (a) an internal register of established breaches of the GDPR and the Personal Data Protection Act, (b) a register of the measures taken in accordance with art. 58, para 2 of the GDPR, and (c) a register of the personal data destroyed on a monthly basis by providers of public electronic communication networks and / or services in accordance with art. 251g of the Electronic Communications Act. These registers, however, are not public.

In accordance with the Rules of Procedure of the Commission for Personal Data Protection and its Administration, the above-mentioned registers are held in electronic format and should be updated regularly.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Personal Data Protection Act does not set an explicit requirement to appoint a data protection officer ("**DPO**"), thus the general requirement pursuant to the GDPR applies. Pursuant to the Personal Data Protection Act, data controllers are obliged to communicate the personal details and contact details of the DPO, as well as any subsequent replacements, before the Commission for Personal Data Protection, and will also have to publish their contact details. An approved notification form, which was recently updated by the Commission for Personal Data Protection, is available online (only in Bulgarian language).

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Personal Data Protection Act does not repeat the core provisions of the GDPR relating to collection and processing of personal data in its body. However, following the direct effect of the GDPR in all EU member states, the provisions of the regulation in this respect shall be applied in all cases of data collection and processing. The Personal Data Protection Act explicitly previews that in case the data subject provides his / her personal data to a data controller or a data processor in breach of Art. 6, para (1) (legal grounds for processing) and Art. 5 (principles for data processing) GDPR, the data controller / data processor should have to immediately return the data or delete / destroy the data within one month of becoming aware of the breach (art. 25a of the Personal Data Protection Act).

The Personal Data Protection Act also introduces additional rules relating to specific data processing situations:

- Conditions applicable to child's consent in relation to information society services – The Personal Data Protection Act introduces a lower age of the data subject, under which the consent of a parent or a guardian would be required for the lawful processing of personal data of a child in cases of direct provision of information society services. Under the Personal Data Protection Act if the data subject is under 14 years old, a consent by a parent exercising the parental rights or by guardian of the data subject is required for the lawful processing of the data.
- Processing of personal identification number – Under the Personal Data Protection Act, public access to personal identification number / personal identification number of a foreigner ('PIN/PINF') shall be granted only if required by law. Data controllers providing electronic services should undertake appropriate technical and organizational measures to prevent the PIN/PINF from being the sole identifier for the use of their services.
- Processing and freedom of expression and information — Where personal data is processed for the exercise of freedom of expression and information, including for journalistic purposes and for the purposes of

academic, artistic or literary expression, the data controller should assess the lawfulness of such processing in each particular case. The Personal Data Protection Act sets a number of assessment criteria to be used by data controllers / processors in the assessment of the lawfulness of processing such as the type of the personal data processed, the impact of the public disclosure on the privacy of the data subject and his / her reputation etc. However, the Bulgarian Constitutional Court (Decision Nr.8 dated November 15,2019) declared the assessment criteria set forth by the Personal Data Protection Act to be unconstitutional. More particularly, the criteria were found to be unclear and therefore creating unpredictability and legal uncertainty and restricting disproportionally the freedom of expression and information. Based on this decision, the above-mentioned criteria do no longer apply. The balancing test between the freedom of expression and the right to information and the protection of personal data shall me made on a case-by-case basis taking into consideration the specific circumstances and interests in presence. Further guidance in this respect was provided in a recent decision of the Supreme Administrative Court (Decision Nr. 11636 dated November 16, 2021), which clarified how the balance between these competing rights shall be assessed in each individual case.

- Processing in the context of employment – The Personal Data Protection Act regulates explicitly certain matters related to personal data processing in the context of an employment relationship. Employers may take copy of employee's identification documents, driving license or residence document only if required by law. In addition, according to a statement by the Commission for Personal Data Protection information for the criminal background of the employees can also be processed by employers only if explicitly provided for by law. Other legal grounds, such as consent or the legitimate interest cannot be applied for the processing of criminal records information. Most recently, the Commission for Personal Data Protection has adopted several opinions concerning the processing of employee health data by employers in the context of Covid-19; in particular, the latter provide that employers:
    - cannot request information from a remote-working employee whether he / she (or any of his / her family members) has tested positive for Covid-19; such information can only be disclosed voluntarily by the employee;
    - may provide anonymized information to their employees about established Covid-19 cases in the company (i.e. without revealing the identity of the infected employee(s));
    - can order / organize Covid-19 group testing of employees, without processing or having access to the test results - since the latter contain sensitive health data, they can only be processed by competent health authorities;
    - may process only aggregated data for the vaccination status of the employees, gathered voluntary and on anonymous basis by the appointed Labour Medicine Office (a third party service provider in the field of occupational medicine, that each employer shall appoint) for the purposes of risk assessment of the health and safety conditions at the workplace.

Employers should adopt rules and procedures for:

- the use of breach reporting system;
- restrictions on the use of internal company resources;
- introduction of systems for control access, working time and labor discipline.

These rules and procedures shall contain information on the scope, obligations and methods with respect to their application. The Personal Data Protection Act recognizes that the business purpose of the employer and the nature of the related work processes shall have to be taken into account upon the adoption of the rules and procedures. The rules and procedures will have to be brought to the attention of the employees.

Employers shall have to further determine a retention period for the personal data collected during the recruitment process, which however may not be longer than six months, unless the candidate consented to a longer period. Where the employer has, for recruitment purposes, requested original or notarized copies of documents certifying the physical and mental fitness of the applicant, the required degree, or the length of service for the previous positions occupied, the employer should return the submitted documents within six months of the conclusion of the recruitment procedure unless otherwise provided by specific law.

- Personal data processing by way of large-scale surveillance of publicly accessible areas – Under the Personal Data Protection Act data controllers and data processors shall adopt internal rules for the processing of personal data through systematic large-scale surveillance of publicly accessible areas, including via video surveillance. These rules should put in place appropriate technical and organizational measures to ensure the protection of data subjects' rights and freedoms. The Personal Data Protection Act provides a definition for 'large-scale' — a systematic monitoring and / or processing of personal data of an unlimited number of data subjects. The rules for personal data processing through large-scale surveillance of publicly accessible areas shall define the legal grounds and objectives for the introduction of a monitoring system, the location, scope and means of monitoring / surveillance, retention periods for the information records and their deletion, the right of review by the persons being subject to surveillance, the means of informing the public about the monitoring carried out, as well as the restrictions on granting access to such information to third parties. The minimum requirements for data controllers / data processors with respect to the aforementioned obligations shall be published on the website of the Commission for Personal Data Protection.

Processing of personal data of deceased persons

The Personal Data Protection Act stipulates, that when processing the personal data of deceased persons data controllers shall have to take appropriate measures to prevent the rights and freedoms of others and the public interest from being adversely affected. In such cases, the data controller may retain the data only if there is a legal basis therefor. In addition, data controllers shall provide upon request access to the personal data of a deceased person, including a copy thereof, to his / her heirs or other persons with legal interest.

The controller shall provide information on action taken without delay and in any event within one month as of the receipt of the request. That period may be extended with two further months where necessary. In case there is a delay, the controller shall provide the reasons for the delay.

Where the request has been made by electronic form, the information shall be provided by electronic means, where possible, unless otherwise requested by the data subject.

If the controller does not act on the request, the controller shall inform without delay and at the latest within one month of receipt of the request of the reasons for not taking action and the possibility of lodging a complaint with a supervisory authority and seeking judicial remedy.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, Korea, the United Kingdom, Eastern Republic of Uruguay and New Zealand. Following the invalidation of the EU – US Privacy Shield by the European Court of Justice, on December 13th, 2022 the European Commission initiated the process to adopt a new adequacy decision for the USA. The draft decision will undergo an EU approval process, including obtaining an opinion from the European Data Protection Board and European Parliament. The European Commission will also need to seek approval of the new adequacy framework from a committee composed of representatives of EU Member States.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The appropriate safeguards include among others binding corporate rules and standard contractual clauses. On 4 June 2021 the

European Commission adopted new set of standard contractual clauses for transfers outside the EU/EEA. Data controllers and processors have term until 27 December 2022 to renegotiate their existing data processing agreements based on the old set of standard contractual clauses in order to reflect the new clauses adopted by the European Commission.

The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The Personal Data Protection Act does not derogate from the provisions of the GDPR regarding data transfer and does not introduce any additional rules or requirements in this respect. Following the direct effect of the GDPR in all EU member states, the provisions of the regulation relating to this matter shall be applied in all cases of data transfer.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The Personal Data Protection Act does not derogate from the provisions of the GDPR regarding security of personal data and does not introduce any additional rules or requirements in this respect.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Personal Data Protection Act does not derogate from the provisions of the GDPR regarding data breach notification and does not introduce any additional rules or requirements in this respect. Following the direct effect of the GDPR in all EU member states, the provisions of the regulation relating to this matter shall be observed. The Commission for Personal Data Protection adopted an internal framework of instructions for evaluation and assessment of submitted data breaches reports, including a methodology for risk assessment in case of established data breaches. The authority further approved a template of data breach notification, which controllers may use. The template is available online in Bulgarian language only.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as

part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The functions of supervision and control of the compliance with the GDPR in Bulgaria are shared between the Commission for Personal Data Protection and the Inspectorate to the Supreme Judicial Council, the latter having competence only with regards to data processing by courts, prosecution offices and criminal investigative bodies in their capacity as judicial authorities.

The competences of the Commission are further defined by reference to art. 57 and 58 of the GDPR. Apart from performing the powers under the GDPR, the Commission is also entitled to:

- analyze and carry out overall supervision and ensure compliance with the GDPR, the Personal Data Protection Act and the legislative acts in the area of personal data protection;
- issue secondary legislation in the area of personal data protection;
- ensure the implementation of the decisions of the European Commission on the protection of personal data and the implementation of binding decisions of the European Data Protection Supervisor;
- participate in international cooperation between data protection authorities and international organizations on personal data protection issues;
- participate in the negotiation and conclusion of bilateral or multilateral agreements on matters within its competence;
- organize, coordinate and conduct training in the field of personal data protection;
- issue administrative acts related to its authority in the cases provided for by law;
- adopt criteria for the accreditation of certification bodies;
- bring proceedings before the court for breach of the GDPR;
- issue mandatory instructions, give instructions and recommendations regarding the protection of personal data;
- impose coercive administrative measures.

The internal Rules of Procedure of the Commission further clarify its tasks, procedures and rules for work of its administration, as well as rules for the proceedings before the Commission.

The Personal Data Protection Act does not derogate from the provisions of the GDPR regarding administrative sanctions, but directly refers to the amounts of fines and pecuniary sanctions set out by the GDPR and the respective criteria for their determination. The Personal Data Protection Act specifies that all sanctions shall be imposed in the BGN equivalent of the EUR amounts set by the GDPR.

For other violations under the Personal Data Protection Act the data controller / data processor shall be subject to a fine or a pecuniary sanction of up to BGN 5000.

A complaint against a decision of the Commission may be withdrawn until the expiry of the period for appealing the said decision. Otherwise, the Commission's decisions are subject to appeal before the Administrative Court Sofia within 14 days of receipt. Decisions of the Administrative Court are subject to appeal before the Supreme Administrative Court which decisions are final.

In case of a violation of his / her rights under the GDPR and the Personal Data Protection Act, every data subject is entitled to refer the matter to the Commission for Personal Data Protection within six months of becoming aware of the breach, but no later than two years from the date of the violation. In addition, data subjects shall be entitled to appeal the actions and acts of the data controller / data processor directly before the administrative courts or the Supreme Administrative Court, except where there are pending proceedings before the Commission for the same matter if a decision regarding the same breach has been appealed and there is not yet a court decision in force. The transfer or distribution of computer or system passwords which results in the illegitimate disclosure of personal data constitutes a crime under the Bulgarian Criminal Code (promulgated in the State Gazette No. 26 of April 2, 1968, as amended periodically) and the penalty for such a crime includes imprisonment for up to three years.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Personal Data Protection Act does not introduce any rules relating specifically to e-marketing. As the legal grounds for processing of personal data under the GDPR are also applicable in the area of e-marketing, the explicit consent of the data subject is likely to be the most suitable ground for the purposes of e-marketing. In certain cases, such processing may also be justified by legitimate interest — according to Recital 47 of the GDPR, direct marketing could be based on legitimate interest, to the extent that: (i) it is targeted only to existing customers; and (ii) the customers can reasonably expect to receive direct e-marketing communications. Still, the possibility to rely on legitimate interest for the purposes of e-marketing would need to be assessed on a case-by-case basis.

In addition, although the repeal of the provision of the Personal Data Protection Act regulating the right of the data subject to object to any data processing for the purposes of direct marketing and does not explicitly refer to the respective provision of the GDPR, following the direct effect of the regulation, data subjects shall still be entitled to object before the data controller or the data processor to their personal data being processed for the purposes of e-marketing.

The Bulgarian Electronic Communications Act explicitly requires, when it comes to direct marketing to natural persons, the opt-in mechanic to be mandatorily applied. After the natural person's consent is provided, the person shall always be given the opportunity to opt out from the direct marketing network and refuse his / her personal data to be further processed for such purposes.

ONLINE PRIVACY

Directive 2002/58 (E-Privacy Directive) is transposed into the Bulgarian Electronic Commerce Act. In 2011 the intention of the legislator was to introduce the amendments of Art. 5(3) under Directive 2009/136. However, the final adopted text still replicates the old wording before Directive 2009/136. The amendment itself was widely interpreted as implementing the text of Directive 2009/136 without, however, introducing the updated text.

Currently, instead of requiring the user's consent, the relevant text in the Electronic Commerce Act states that users should be provided with clear and comprehensive information in accordance with Art.13 of the GDPR and they must be given the opportunity to refuse the storage or access to such information (i.e. opt-out regime).

KEY CONTACTS

Wolf Theiss

www.wolftheiss.com/

Anna Rizova
Partner
Wolf Theiss
T +359 2 8613703
anna.rizova@wolftheiss.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BURKINA FASO

Last modified 8 January 2024

LAW

The data protection regime in Burkina Faso is governed by the following laws and regulations:

- Law No. 001-2021 of March 30, 2021 on the protection of persons with regard to the processing of personal data.
- Law 010-2004/AN on the protection of personal data.
- Decree No. 2007-283/PRES/PM/MPDH of 18 May 2007 regarding the organisation and functioning of the Commission de l'Informatique et des Libertés;
- Decree No. 2007-757/PRES/PM/MPDH/MEF appointing the members of the Commission de l'Informatique et des Libertés ; and
- Order No. 2008/001/CIL fixing the internal regulations of the Commission de l'Informatique et des Libertés.

The Burkina Faso has also adopted on 22 November 2013 the Marrakech resolution issued by the French-speaking association of data protection authorities relating to the procedure for the supervision of personal data transfers of personal data in the French-speaking world by means of binding corporate rules.

DEFINITIONS

Definition of Personal Data

Any information that allows, in any form whatsoever, directly, or indirectly, the identification of natural persons, in particular by reference to an identification number or to several characteristics specific to their physical, psychological, mental, economic, cultural or social identity (Article 5 of the Law).

Definition of Sensitive Personal Data

Any personal data relating to the data subject's health or that reveal racial or ethnic origins, political, philosophical or religious opinions, union membership, morals, investigation and prosecution of offenders, criminal or administrative penalties, related security measures or other measures of a similar nature (Article 5 of the Law).

NATIONAL DATA PROTECTION AUTHORITY

The Burkina Faso's data protection authority is the Commission de l'Informatique et des Libertés ('**CIL**').

The CIL draws its membership from various segments of society. It is charged with:

- making individual or regulatory decisions in cases provided for under the law;
- assisting with data processing inspections and obtaining all information and documents needed for its mission;
- issuing model rules to ensure security; and where appropriate, prescribing safety measures including the destruction of information;

- issuing enforcement notices to data controllers and sharing with the prosecutor’s office the offenses of which the body is aware;
- ensuring that the implementation of the right of access and rectification indicated in the acts and declarations do not impede the free exercise of this law;
- receiving complaints and petitions;
- staying informed of the latest technological developments, and keeps abreast of their effects on the right to the protection of privacy, the exercise of freedoms, and the functioning of democratic institutions;
- advising individuals and organisations that use automated processing, or who carry out tests or experiments likely to lead to such processing;
- responding to requests for public opinion; and
- proposing legislation or regulations to the Government to adapt the protection of freedoms to technological evolution.

REGISTRATION

The is no country-wide system of registration in Burkina Faso. However, the law imposes an obligation of notification and annual reporting to the National Data Protection Authority. These annual reports provide information on those responsible of personal data's activity throughout the concerned year.

DATA PROTECTION OFFICERS

We have not identified any obligation to appoint a data protection officer ('**DPO**') or any other equivalent role in the law.

COLLECTION & PROCESSING

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. These include:

- **consent and legitimacy:** unless otherwise provided by law, data controllers are obligated to obtain consent from the data subject;
- **purpose:** personal data can only be collected and processed for a specific and legitimate purpose;
- **proportionality and relevance:** personal data must only be processed in a relevant and necessary manner regarding the purpose and objectives of the processing;
- **lawfulness and fairness:** data controllers must collect and process data in a fair, lawful, and not fraudulent manner
- **data retention:** a specified period of time should be determined in advance depending on the purpose of processing to ensure that personal data is not stored indefinitely;
- **security and confidentiality:** all responsible persons for processing personal data must not only ensure the security of data or files to prevent their destruction, or alteration; but also prevent unauthorised access to personal data contained in a file or intended to form part of the files;
- **preliminary formalities:** without exception or exemption provided by law, all data controllers shall, depending on the nature of personal data processing, namely notify the CIL or ask his opinion or obtain approval, etc.

Except where provided otherwise by the law, any processing of personal data shall be carried out with the express consent of the data subject(s).

The processing of personal data can legally be carried out without the consent of the data subject(s), when it is necessary for:

- the performance of a contract to which the data subject is a party; or
- pre-contractual measures taken at the request of the data subject;
- compliance with a legal obligation to which the controller is subject and when the processing is essential to protect the life of the data subject or that of a third party;
- the purposes of preventive medicine, medical diagnosis, the administration of care or treatment, or the management of health services, provided that it is carried out by a member of a health profession or by another person who, by reason of his / her duties, is bound by professional secrecy;

- the establishment of an offence, a right, or the exercise or defence of a right in a court of law and when the said processing relates to data made public by the data subject.

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller. It may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Data subjects may request erasure of their personal data. It has the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

Unless an authorisation is required, the law provides that controllers should notify all processing to the CIL. The following are exempt from the notification requirement to CIL:

- temporary copies that are made as part of the technical activities of transmission and provision of access to a digital network for the purpose of automatic intermediate and transitory storage of data for the sole purpose of allowing other recipients of the service the best possible access to the information;
- processing carried out by a natural person for the exercise of exclusively personal or domestic activities;
- disclosed to third parties and not used to support actions or decisions against an individual;
- automated processing of personal data for the purpose of research in the field of health;
- automated processing of personal data carried out on behalf of the State, a public institution, a local authority or a legal person under private law managing a public service.

With respect to day-to-day processing of data which do not infringe on privacy or freedoms, the Law provides that the CIL establishes and publishes 'simplified norms,' which shall include certain information, including:

- the date of the declaration;
- the full name and address or the name and headquarters of the person making the request and the person who has the power to decide on the creation of the data processing (data controller) or, if he or she resides abroad, his or her representative in Burkina Faso;
- the characteristics, purpose and, if applicable, the name of the data processing operation;
- the department or departments responsible for carrying out the processing;
- the department to which the right of access is to be exercised and the measures taken to facilitate the exercise of this right
- the categories of persons who, by reason of their functions or for the needs of the service, have direct access to the information recorded;
- the personal information processed, its origin and the length of time it is kept, as well as the recipients or categories of recipients authorized to receive this information;
- the reconciliation, interconnection or any other form of linking of this information as well as its transfer to third parties;
- the measures taken to ensure the security of data and information processing and the guarantee of secrets protected by law;
- if the data processing is intended for the dispatch of personal data between the territory of Burkina Faso and abroad in any form whatsoever, including when it is the object of operations partially carried out on the territory of Burkina Faso from operations previously carried out outside Burkina Faso.

When processing complies with a simplified norm issued by the CIL, no authorisation or notification is required, but only a 'simplified declaration of conformity,' to the said norm is required. The simplified declaration of conformity shall be sent to the CIL. Unless otherwise decided by the CIL, a receipt is issued without delay after the simplified declaration of conformity has been sent to the CIL. As from receiving this receipt, the applicant can start carrying out the processing.

Except in cases where they are to be authorised by law, automated processing of personal data carried out on behalf of the State, or on behalf of any public institution, local authority, or on behalf of a private legal person operating a public service, must be authorised by decree after the CIL's approval. In the case of a negative opinion by the CIL, an appeal can be lodged to the Administrative Supreme Court *(Conseil d’Etat).*

TRANSFER

The provisions of the Law pertaining to international transfers are broadly drafted.

According to said provisions, international transfers cannot be made without the respect of the following conditions:

- To request the authorisation of the CNIL;
- To sign with the contracting party, a data confidentiality clause and a data reversibility clause in order to facilitate the complete migration of the data at the end of the contract;
- Implement technical and organisational security measures.

Additionally, the transfer can only be made to a foreign country or an international organisation if the beneficiary country or international organisation ensures an adequate level of protection equal to the one ensured in Burkina Faso (Article 42 of the law).

As a signatory to the Marrakech Resolution of 22 November 2013, Burkina Faso recognizes the application of the French-speaking RCE, which consist in a code of conduct by which a group of companies defines its internal policy on the transfer of personal data. The RCE are based and designed on the model of the European Commission’s binding corporate rules ('**BCR**').

In practice, the RCE mechanism concerns the authorities of the AFAPDP member countries that have adopted the cooperation protocol and the resolution on the framework for data transfers in the French-speaking area. These concerns at least the following 13 countries: Albania, Andorra, Belgium, Benin, Burkina Faso, France, Gabon, Luxembourg, Mauritius, Morocco, Senegal, Switzerland and Tunisia.

The RCE cover intra-group transfers of personal data carried out by a company established in an AFAPDP member country, to other companies of the group, whether the latter are located in an AFAPDP member country or not.

SECURITY

The personal data Act is not prescriptive about specific technical standards or measures.

However, the Article 24 states that the data controller shall take all necessary measures in view of the nature of the data and the architecture of the processing, in particular to prevent them from being distorted, damaged, lost, stolen or accessed by unauthorised parties.

BREACH NOTIFICATION

Not applicable.

Mandatory breach notification

We have not identified, in the law, any general obligation to notify the data subject in the case of a security breach. However, Article 21 of the law provides that in the event where 'information has been transmitted by mistake to a third party, its rectification or cancellation shall be notified to that third party, unless an exemption is granted by the control authority' (i.e. the CIL).

ENFORCEMENT

The law empowers the CIL to impose various sanctions depending on the severity of the infringement. However, the level of enforcement remains quite low due to resource limitations and the fact that this field of law is still new to the administration and business and data subjects.

The CIL may, directly or through an expert authorized for this purpose, carry out checks and controls on any processing of personal data.

However, if the data controller initiates the inspection, he or she must pay the inspection fees, the amount of which is set by order of the Minister of Finance.

On completion of its checks and inspections, the CIL may impose the following administrative sanctions on offenders, without prejudice to criminal prosecution:

- a warning;
- formal notice;
- injunction to cease data processing;
- blocking of certain personal data;
- lump-sum fines;
- withdrawal of authorization.

The amount of the fine is proportionate to the seriousness of the breaches committed and to the benefits derived from the breach.

The sanctions provided for by law are imposed on the basis of a report drawn up by one of the members of the CIL, appointed by the Chairman. This report is sent to the data controller, who may submit observations and be represented or assisted at a hearing before the CIL.

The amount of the fixed fine provided for by law is proportionate to the seriousness of the breaches committed and the benefits derived from the breach. For the first offence, the fine is one percent of sales excluding tax for the last financial year for which the accounts have been closed. In the event of a repeat offence, the fine is five percent of sales excluding tax for the last financial year for which the accounts have been closed. Fixed-rate fines are recovered as receivables from the State.

Financial penalties may also be imposed on any data controller, ranging from XOF five million (5,000,000) to XOF one hundred million (100,000,000).

Sanction by the data protection Authorities may be appealed before the competent administrative court.

ELECTRONIC MARKETING

The personal data Act will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name).

The general rule for electronic marketing is that it requires the express consent of the recipient (see Article 49 of law No. 045-2009/AN of November 10, 2009 regulating electronic services and transactions in Burkina Faso and Article 14 of the personal data Act).

Even when a marketer has the consent of a data subject, that consent can be withdrawn by the data subject under Article 20 of the Personal Data Act.

The data subject has the right to object at any time to the use of his / her personal data for such marketing.

This right to object must be explicitly brought to the attention of the data controller.

However, the data controller may not respond favourably to a request to exercise the right to object if it demonstrates the existence of legitimate reasons justifying the processing, which override the interests, fundamental rights and freedoms of the data subject.

ONLINE PRIVACY

The Law does not provide any specific rules governing cookies and location data.

However, pursuant to Article 10 of the data controller must implement all appropriate technical and organisational measures to preserve the security and confidentiality of the data, including protecting the data against accidental or unlawful destruction, accidental loss, alteration, distribution or access by unauthorised persons.

KEY CONTACTS

Geni & Kebe
www.dlapiperafrica.com/senegal

Dr. Francky Lukanda
Senior Associate
Geni & Kebe
T +2250584344660
f.lukanda@gsklaw.sn

Mouhamed Kebe
Managing Partner
Geni & Kebe
T +221 76 223 63 30
mhkebe@gsklaw.sn

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

BURUNDI

Last modified 17 January 2024

LAW

Burundi does not have a law that specifically regulates personal data protection. However, several laws and regulations currently in force contain data protection provisions or impose confidentiality obligations on specific types of personal information. For example, employment, banking, telecommunications and health sector laws impose some data protection requirements. Such provisions generally require covered entities to maintain the confidentiality of personal information.

- Article 2, point 8 of LAW N°1/10 OF MARCH 16, 2022 ON THE PREVENTION AND REPRESSION OF CYBERCRIMINALITY IN BURUNDI defines personal data as any information of any kind, regardless of medium, including sound and image, relating to an identified or identifiable natural person, directly or indirectly, by reference to an identification number or to one or more factors specific to his or her physical, physiological, genetic, mental, cultural, social or economic identity. This law provides for sanctions against individuals (articles 61, 62 ,63) and service providers or any network operator (articles 14,15);
- Under Law no. 1/07 of march 12, 2020 amending Law n° 1/012 of May 30, 2018 on the Code of Health Care and Health Services Provision in Burundi, healthcare institutions are required to maintain the confidentiality of patient information, unless confidentiality is waived in cases provided for by law;
- Law No. 1/17 of August 22, 2017 governing banking activities: Article 133 imposes confidentiality obligations on customer and account information. This article provides that any person who contributes to the operation, control or supervision of a banking institution is bound to professional secrecy. Violations are enforced under penal code provisions without prejudice to disciplinary proceedings;
- Under Law n°1/11 of November 24, 2020 revisioning decree-law n°1/037 of 07/07/1993 revisioning the labor code of Burundi, labor and social security inspectors, their agents, as well as persons having participated in any capacity whatsoever in any controls, examinations or investigations in collaboration with the labor and social security inspector are bound by professional secrecy (article 430);
- Several Ministerial Orders applicable to the telecommunications sector have been adopted to protect the privacy of and restrict access to and interception of the contents of communications (Legislative Decree No. 100/153 of June 17, 2013 on the Regulation of the Control and Taxation System for International Telephone Communications entering Burundi; Decree-Law No. 100/112 of April 5, 2012 on the Reorganization and Operation of the Telecommunications Regulatory and Control Agency 'ARCT'; Ministerial Ordinance No. 730/1056 of November 7, 2007 on the interconnection of telecommunications networks and services opened to the public).

DEFINITIONS

Definition of personal data

Not specifically defined.

Definition of sensitive personal data

Not specifically defined.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in Burundi.

REGISTRATION

There is no requirement to register databases.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

Most sector specific laws and regulations that impose confidentiality and data protection requirements apply to covered entities under the law or regulation, and require such entities to maintain the confidentiality of personal information during processing.

TRANSFER

No geographic transfer restrictions apply in Burundi. Certain sector specific provisions require companies to obtain consent prior to third party transfers of personal information. Notably, under Article 16 of Law n ° 1/012 of May 30, 2018 on the Code of Health Care and Health Services Provision in Burundi, "every patient has the right to decide on the use of the medical information concerning him and the conditions under which they may be transmitted to third parties."

SECURITY

There are no specific data security requirements in Burundi.

BREACH NOTIFICATION

There are no breach notification requirements in Burundi.

ENFORCEMENT

The relevant sector specific agency or regulator is generally authorized to enforce violations of confidentiality requirements.

ELECTRONIC MARKETING

There are no specific electronic marketing requirements in Burundi.

ONLINE PRIVACY

There are no specific online privacy requirements in Burundi.

KEY CONTACTS

Claver Nigarura
Managing Partner
Rubeya & Co-Advocates
T +257 22 24 89 10
claver@rubeya.bi

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CAMBODIA

Last modified 18 January 2024

LAW

The Ministry of Post and Telecommunications (**MPTC**) announced on 19 February 2021 their intention to prepare a comprehensive personal data protection law after finalizing the draft cybersecurity law.

On 22 December 2021, the Royal Government of Cambodia issued Sub-Decree No. 252 on the Management, Use, and Protection of Personal Identification Data (only available in Khmer) (Sub-Decree 252) in order to promote broad policy objections, such as:

- ensuring the protection of peace and order;
- serving the public interest; and
- promoting national development by improving the provision of services.

However, Sub-Decree 252 only applies to "personal identification data" owned by the Ministry of Interior (MOI) and does not apply to personal identification data used by other entities.

In September 2023, the MPTC made available to select private organizations and companies a Draft Law on Personal Data Protection for their review and comment. However, it has not been made available to the public as of writing. Therefore, the information provided regarding the data protection law should be used as a reference and not considered final, as the draft law has not been officially released to the public. The Draft Law on Personal Data Protection establishes rules, principles, and mechanisms to govern the collection, use, and disclosure of personal data. Its main objective is to safeguard the privacy rights of individuals and encourage the lawful and responsible use of personal data.

The E-Commerce Law contains provisions for the protection of consumer data that has been gathered over the course of electronic communications. The E-Commerce Law is thereby restricted in scope to virtual and / or digital data protection.

Other matters pertaining to data protection typically fall under the right to privacy, which is protected in broad terms under the Constitution of the Kingdom of Cambodia 2010, the Civil Code of the Kingdom of Cambodia 2007, the Criminal Code of the Kingdom of Cambodia 2009, the Code of Criminal Procedure of the Kingdom of Cambodia 2010, and other specific laws such as the Banking Law.

DEFINITIONS

Definition of Personal Data

Cambodian law does not specifically define the term "personal data," or discuss what specific information constitutes personal data.

The E-commerce Law defines the term "data" as "a group of numbers, characters, symbols, messages, images, sounds, videos, information or electronic programs that are prepared in a form suitable for use in a database or an electronic system".

According to the Draft Law on Personal Data Protection, personal data is defined as information pertaining to an individual that can directly or indirectly identify them. This information includes, but is not limited to, names, identification numbers, location data, and online identifiers. As the Law on Personal Data Protection has not yet been implemented, this definition should not be regarded as official.

Therefore, due to the absence of a definition of "personal data", it remains plausible that any data of a data subject may be viewed by the regulatory and enforcement authorities as personal data of that data subject. As such, conventional data, such as full names, national identification numbers, passport numbers, photographs, video, images, phone numbers, personal email addresses, biometric data, IP addresses, and other network identifiers, etc., may arguably constitute personal data.

Definition of Sensitive Personal Data

There is no express definition of what constitutes sensitive personal data. That said, based on laws applicable to persons and entities in other sectors (such as healthcare and banking), the types of data below are generally considered to be of a more sensitive nature, and thus should be handled with more stringent data protection mechanisms:

- medical data;
- financial data;
- personal data of children; and
- personal identifiers (e.g. national identification cards and passport details).

As there is no clear limit as to the scope of what may be considered sensitive data, any data of a data subject should be prudently treated as sensitive data to the greatest extent possible.

NATIONAL DATA PROTECTION AUTHORITY

Since Cambodia does not have any dedicated laws on data protection, there are no regulatory or enforcement authorities that are specifically tasked with handling, overseeing or implementing personal data protection matters in Cambodia.

That said, the following governmental bodies may have substantial powers over data protection matters:

- the Ministry of Commerce (“**MOC**”);
- the Ministry of Post and Telecommunications (“**MPTC**”); and
- the Ministry of Interior (“**MOI**”).

REGISTRATION

Since Cambodia does not have any dedicated laws on data protection, there are no specific registration requirements for data protection. However, “Electronic Commerce Service Providers” and “Intermediaries” (in an e-commerce context), who would likely store, process and transfer the data of the data subjects, must register with the MOC and MPTC.

Under the E-Commerce Law, “Electronic Commerce Service Providers” are defined as persons who use electronic means to supply goods and / or services, except insurance institutions, and an “Intermediary” is broadly defined as a person who provides services of sending, receiving, transmitting or storing, either on a temporary or permanent basis, electronic communications, or other services relating to electronic communications, including persons who represent the originators; persons providing means of seeking any data in an electronic system; persons providing online marketing and online commercial services; and other persons as specified under the E-Commerce Law.

DATA PROTECTION OFFICERS

Since Cambodia does not have any dedicated laws on data protection, there are no specific requirements in Cambodia to appoint data protection officers who are specifically tasked with handling, overseeing or implementing data protection matters in Cambodia.

COLLECTION & PROCESSING

As Cambodia has not enacted any dedicated or comprehensive data protection laws, there are no laws or regulations in Cambodia that explicitly and specifically discuss the concept of collection and processing of data.

However, under the Draft Law on Personal Data Protection, the term “data controller” is defined as a natural person, private legal entity, public establishment of administrative character, or public entry that determines the purpose and means of collecting, using, or disclosing personal data. On the other hand, a “data processor” is defined as a natural person, private legal entity, public establishment of administrative character, or public entry that processes personal data on behalf of a data controller or public authority.

Based on Cambodia’s existing legal framework for data privacy, seven data protection obligations are either implied or explicitly imposed. Those obligations are discussed below.

1. Consent Obligation: There is no explicit statutory requirement to obtain consent, or penalty for failing to obtain such consent under Cambodian law when collecting and processing of data. However, the Civil Code and several other pieces of legislation indicate that there is a general recognition of the protection of the right to privacy and the obligation to protect data from unauthorized access. That being said, under a conservative approach, an organization may decide to obtain consent from a data subject before collecting, using, or disclosing personal data for a purpose in order to completely minimize future risks. Organizations should allow an individual who previously gave consent to withdraw his / her consent.
2. Purpose Limitation Obligation: Collect, use, or disclose personal data about an individual only for purposes that are reasonable and that have been disclosed / notified to the individual concerned.
3. Disclosure / Notification Obligation: Disclose to or notify the individual of the purpose(s) for which the organization intends to collect, use or disclose the individual’s personal data on or before such collection, use or disclosure of the personal data. The purposes notified must be reasonable.
4. Correction Obligation: Correct any incorrect or inaccurate personal data of a data subject that is in the possession or under the control of the organization upon request of the data subject.
5. Access Obligation: Allow data subjects to access their personal data in the possession or under the control of an organization for correcting the information under the Correction Obligation.
6. Protection Obligation: Protect personal data in its possession or under its control by taking necessary measures to prevent loss, unauthorized access, use, alteration, leak, disclosure, or otherwise.
7. Retention Obligation: Retain all personal data that is in its system, and that may give rise to civil and criminal liability.

The Draft Law on Personal Data Protection also supports these general principles and stipulates that the principles of personal data protection include:

- lawfulness, fairness, and transparency;
- purpose limitation;
- accuracy of personal data;
- retention limitation;
- security safeguards; and
- accountability.

TRANSFER

While Cambodia does not have comprehensive data protection legislation that explicitly prohibits an organization from transferring data, there is a general recognition of the protection of the right to privacy and the obligation to protect data from unauthorized access under the Civil Code and several pieces of legislation, although none of them imposes or implies any restrictions on the transfer of data. Therefore, personal data should only be collected, used, or disclosed for purposes that the individual understands and has given consent to at the time of giving initial consent or a new consent. Such purposes should be disclosed or notified to data subjects in a reasonable manner based on the circumstances.

Where the use and disclosure of the personal data is for a purpose different from that for which it was initially collected, it is recommended to notify the individual of the new purpose and obtain a new consent unless:

- the new purpose is within the scope of the original consent; or
- implied consent can be established.

Implied consent refers to any act that is generally recognized as consent under applicable trade practices. However, it is recommended that a new consent that is express and written be obtained once service providers use or disclose personal data for a purpose different from that for which it was collected.

When a service provider is seeking consent from the data subject, the service provider should disclose or notify the data subjects of the purpose(s) for which it intends to collect, use or disclose the data subjects' personal data before such collection, use or disclosure of the personal data. Cambodia's laws related to data protection do not prescribe how an organization should notify individuals. Organizations must determine what would be the most appropriate form of notification. The form of the disclosure / notification to obtain each data subject's consent should be as close to a formal contract as possible. Moreover, requirements such as clicking on the consent button, typing a full legal name for the signature, and / or scrolling through all terms of the disclosure / notification should be implemented. Furthermore, disclosures / notifications to the individuals regarding the purpose of the collection, use, and disclosure of personal data must not be too vague or broad in scope; an appropriate level of specificity should be provided.

In addition to laws of general application, the Draft Law on Personal Data Protection specifically mandates the requirement of consent for the collection, use, or disclosure of personal data. Furthermore, consent for the collection, use, or disclosure of personal data is only considered valid if the data controller provides notification to the data subject and the data subject gives their consent for that specific purpose.

Therefore, where the organization will be disclosing or transferring personal data to third parties, the organization should notify the individuals of such disclosure or transfer. Any consent provided by the individual without first being disclosed or notified of the purposes would not be valid.

SECURITY

Article 32 of the E-Commerce Law directly addresses matters of data protection in the course of electronic communication.

Service providers that electronically store consumers’ private information must take all reasonable security measures to avoid loss, modification, leakage, and / or unauthorized disclosure of all consumer data. The E-Commerce Law notes, however, that disclosures are allowable with the consent of authorities, or with the consent of the individual whose data is being disclosed. The E-Commerce Law does not provide specific guidelines as to how or what mechanisms are required. It is simply required that any measures could be used as long as they could reasonably protect the data from loss, or unauthorized access, use, alteration, or disclosure without authorization or illegally.

The E-Commerce Law also prohibits any encryption of data that may be used as evidence for any accusation or offence. This obligation potentially allows governmental authorities to order the decryption of data implicated in an investigation.

The E-Commerce Law also makes a blanket prohibition on certain forms of cybercrime, including interference with any electronic system for the purpose of accessing, downloading, copying, extracting, leaking, deleting, or otherwise modifying any stored data in bad faith or without authorized permission.

Article 47 of the Banking Law prohibits those who participate in the administration, direction, management, internal control, or external audit of a covered entity, and employees of the latter from providing confidential information pertaining to statements, facts, acts, figures, or the contents of accounting or administrative documents of which they might have become aware through their functions. However, this professional secrecy obligation cannot be used as a ground for nondisclosure in relation to requests by supervisory authorities, auditors, provisional administrators, liquidators, or a court dealing with criminal proceedings.

In case the service provider is not under the scope of the E-Commerce Law or Banking Law, the obligations under the laws of general application that require protection of the right to privacy and the obligation to protect data from unauthorized access should apply when a service provider collects, uses, discloses and processes data of the subject.

Furthermore, the Draft Law on Personal Data Protection requires the data controller to protect personal data under its possession or control by setting up a security system to prevent unauthorised access, collection, use disclosure, copying, modification or disposal, or similar risks; and the loss of any storage medium or device on which personal data is stored. The data processor must also take security measures to prevent loss or unauthorised or unlawful access, use, modification, or disclosure of personal data.

BREACH NOTIFICATION

Currently, there is no breach notification requirement under Cambodian law. However, it is anticipated that the requirement for data controllers and data processors to notify the competent authority and the affected data subjects will be enforced once the Draft Law on Personal Data Protection comes into effect.

ENFORCEMENT

Since there are no regulatory or enforcement authorities that are specifically tasked with handling, overseeing or implementing personal data protection matters in Cambodia, the enforcement of the data protection would generally fall under the auspice of authorities across various sectors:

- the Ministry of Commerce;
- the Ministry of Post and Telecommunications; and
- the Ministry of Interior.

ELECTRONIC MARKETING

Since Cambodia does not have any dedicated laws on data protection, there are no special requirements when obtaining consent for marketing purposes. The E-commerce Law suggests that it is not necessary to obtain consent from the individual to send marketing communications as long as each marketing communication has clear and straightforward opt-out instructions and the individual has not previously exercised his / her opt-out right. Electronic marketing in Cambodia is subject to the general laws relating to digital marketing issues including:

- Law on Consumer Protection, which prohibits "unfair practices" in relation to consumer transactions. Unfair practices include unfair sales; bait advertising; unfair solicitation sales; demanding or accepting payments without intention to supply goods or services per the purchase order; making a false claim or representation of some business activity; coercion by force and mental threats; pyramid schemes; selling goods bearing a false trade description; and any other unfair practices.
- Law Concerning Marks, Tradenames and Acts of Unfair Competition, is relevant to comparative advertising. The following acts are considered acts of unfair competition: all acts that create confusion with the establishment, the goods, or the industrial, commercial or service activities of a competitor; false allegations in the course of trade of such a nature as to discredit the establishment, the goods, or the industrial, commercial or service activities of a competitor; and indications or allegations of the use of marks which, in the course of trade, misleads the public as to the nature, manufacturing process, characteristics, suitability for their purpose, or quantity of the goods.
- Telecommunications Law, which prohibits all activities against the principles of fair, free, equal, and effective competition.
- Other regulations on the Management of Advertisement on Website, Social Network, Mass Media and Mobile Phone Operators.

ONLINE PRIVACY

As mentioned under the Collection and Processing and Transfer sections, under a conservative approach, personal data should only be collected, used, or disclosed for purposes that the individual understands and has given consent to at the time of giving

initial consent or a new consent. Such purposes should be disclosed or notified to data subjects in a reasonable manner based on the circumstances. That said, to minimize future risks, any personal data, including location data, should only be collected and shared online through website cookies after the organization obtains consent from the data subject.

For obtaining consent from the data subject, please refer to the Transfer section.

KEY CONTACTS

Jay Cohen
Partner and Director of Cambodian Office
Tilleke & Gibbins (Cambodia) Ltd
T (+855) 17 87 57 238
jay.c@tilleke.com

Sochanmalisphoung Vannavuth
Associate
Tilleke & Gibbins (Cambodia) Ltd
T (+855) 10 61 65 91
sochanmalisphoung.v@tilleke.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CANADA

Last modified 26 January 2023

LAW

In Canada there are 28 federal, provincial and territorial privacy statutes (excluding statutory torts, privacy requirements under other legislation, federal anti-spam legislation, criminal code provisions etc.) that govern the protection of personal information in the private, public and health sectors. Although each statute varies in scope, substantive requirements, remedies and enforcement provisions, they all set out a comprehensive regime for the collection, use and disclosure of personal information.

The summary below focuses on Canada’s private sector privacy statutes:

- Personal Information Protection and Electronic Documents Act ('PIPEDA')
- Personal Information Protection Act (Alberta) ('PIPA Alberta')
- Personal Information Protection Act (British Columbia) ('PIPA BC')
- Act Respecting the Protection of Personal Information in the Private Sector ('Quebec Private Sector Act'), (collectively, 'Canadian Privacy Statutes')

On June 16, 2022, the federal Government introduced Bill C-27, a wide-reaching piece of legislation that is intended to modernize and strengthen privacy protection for Canadian consumers and provide clear rules for private-sector organizations. It is the second attempt to modernize federal private-sector privacy legislation, after a previous proposal died on the order paper in 2021. If adopted, Bill C-27 will replace PIPEDA with legislation specific to consumer privacy rights (the *Consumer Privacy Protection Act*) and electronic documents (the *Electronic Documents Act*). Bill C-27 will also introduce the *Artificial Intelligence and Data Act*, which aims to create rules around the deployment of AI technologies.

Key elements of Bill C-27 include:

- Clarified consent requirements for the collection, use and disclosure of personal information
- Expanded enforcement powers for the Office of the Privacy Commissioner of Canada, including stiff penalties for serious offenses of up ‎to 5% of annual gross global revenue or CA$25 million
- New rules governing de-identified information
- The creation of a specialized Personal Information and Data Protection Tribunal

C-27 is currently at the committee stage of the legislative process. There has been considerable debate over the Bill, in particular over the proposed *Artificial Intelligence and Data Act.* The final form of the language remains subject to material change.

PIPEDA applies to all of the following:

- Consumer and employee personal information practices of organizations that are deemed to be a ‘federal work, undertaking or business’ (*eg*, banks, telecommunications companies, airlines, railways, and other interprovincial undertakings)

- Organizations who collect, use and disclose personal information in the course of a commercial activity which takes place within a province, unless the province has enacted ‘substantially similar’ legislation (PIPA BC, PIPA Alberta and the Quebec Private Sector Act have been deemed ‘substantially similar’)
- Inter provincial and international collection, use and disclosure of personal information in connection with commercial activity

PIPA BC, PIPA Alberta and the Quebec Private Sector Act apply to both consumer and employee personal information practices of organizations within BC, Alberta and Quebec, respectively, that are not otherwise governed by PIPEDA.

Quebec recently enacted a major reform of its privacy legislation with the adoption of Bill 64. Bill 64 received Royal Assent on September 22, 2021. A first set of amendments came into force on September 22, 2022, with additional modifications set to come into force on September 22, 2022, while the majority of substantial changes came into force on September 22, 2023. A third, more limited set of amendments will come into force on September 22, 2024. With Bill 64’s changes, Quebec now has in place a sophisticated legal framework for privacy and data protection that resembles the European GDPR in several key areas.

DEFINITIONS

Definition of personal data

‘Personal information’ includes any information about an identifiable individual (business contact information is expressly “carved out” of the definition of ‘personal information’ in some Canadian privacy statutes).

The Quebec Private Sector Act, as modified by Bill 64, has broadened the definition of “personal information” to include any information that allows an individual to be identified indirectly as well as directly. In Quebec, business contact information is included in the definition of “personal information”, however it is considered a less sensitive form of data to which many of the requirements of the Quebec Private Sector Act do not apply.

Definition of sensitive personal data

Not specifically defined in Canadian Privacy Statutes, except for the Quebec Private Sector Act.

The Quebec Private Sector Act, as modified by Bill 64, defines ‎‎“sensitive personal information” as any information ‎that, by virtue of its nature (e.g. biometric or medical), or because of the context in which it is used or communicated, warrants a high expectation of privacy. The Quebec Privacy Act has stricter consent requirements in certain situations for the use and communication of personal information qualified as sensitive.

Definition of anonymized information

The Quebec Private Sector Act, as modified by Bill 64, defines “anonymized information” as information concerning an individual which irreversibly no longer allows such individual to be identified, whether directly or indirectly. Quebec recently adopted a regulation which prescribes certain criteria and procedures which must be followed when anonymizing data.

Definition of de-identified information

The Quebec Private Sector Act, as modified by Bill 64, defines “de-identified information” as any information which no longer allows the concerned individual to be identified directly. “De-identified” information is still considered to be a form of personal information, to which most of the protections set out in the Quebec Private Sector Act continue to apply.

Definition of biometric information

The Quebec privacy regulator, the *Commission d’accès à l’information* (CAI), defines “biometric information” as information measured from a person’s unique physical, behavioural or biological characteristics. Biometric information is, by definition, sensitive information.

NATIONAL DATA PROTECTION AUTHORITY

Office of the Privacy Commissioner of Canada ('PIPEDA')‎

Office of the Information and Privacy Commissioner of Alberta ('PIPA Alberta')‎

Office of the Information and Privacy Commissioner for British Columbia ('PIPA ‎BC'), and

Commission d’accès à l’information du Québec (the “CAI”) ('Quebec Private Sector Act')‎

REGISTRATION

There is no general registration requirement under Canadian Privacy Statutes.

Some registration requirements exist under Quebec privacy laws:

- Personal information agents, defined as “any person who, on a commercial basis, personally or through a representative, establishes files on other persons and prepares and communicates to third parties credit reports”, must be registered with the CAI
- The use of certain biometric systems and the creation of databases of biometric information must be disclosed to and registered with the CAI

DATA PROTECTION OFFICERS

PIPEDA, PIPA Alberta, and PIPA BC expressly require organizations to appoint an individual responsible for compliance with the obligations under the respective statutes.

The Quebec Private Sector Act, as modified by Bill 64, requires organizations to appoint a person responsible for the protection of personal information, who is in charge of ensuring compliance with privacy laws within the organization. By default, the person with the highest authority within the organization will be the person responsible for the protection of personal information, however this function can be delegated to any person, including a person outside of the organization.

This person’s responsibilities are broadly defined in the law and include:

- Approval of the organization’s privacy policy and ‎practices
- Mandatory privacy impact assessments
- Responding to and reporting security breaches, and
- Responding to and enacting access and ‎rectification rights

The contact information of the person responsible for the protection of personal information must be published online on the website of the organization.

COLLECTION & PROCESSING

Canadian Privacy Statutes set out the overriding obligation that organizations only ‎collect, use and disclose personal information for purposes that a reasonable person ‎would consider appropriate in the circumstances.‎

Subject to certain limited exceptions prescribed in the Acts, consent is required for the ‎collection, use and disclosure of personal information. Depending on the sensitivity of ‎the personal information, consent may need to be presented as opt-in or opt-out. Under the Quebec Private Sector Act, consent must be “clear, free and informed and be given for specific

purposes”: this is generally interpreted as requiring opt-in consent in most situations, however depending on the context and sensitivity of the information, opt-out or implicit consent may, in certain specific situations, be considered valid. Organizations must limit ‎the collection of personal information to that which is necessary to fulfil the identified ‎purposes and only retain such personal information for as long as necessary to fulfil the ‎purposes for which it was collected.‎

Each of the Canadian Privacy Statutes have both notice and openness/transparency ‎requirements. With respect to notice, organizations are generally required to identify ‎the purposes for which personal information is collected at or before the time the ‎information is collected. With respect to openness/transparency, generally Canadian ‎Privacy Statutes require organizations make information about their personal ‎information practices readily available.‎

All Canadian Privacy Statutes contain obligations on organizations to ensure personal ‎information in their records is accurate and complete, particularly where the information ‎is used to make a decision about the individual to whom the information relates or if the ‎information is likely to be disclosed to another organization.‎

Each of the Canadian Privacy Statutes also provides individuals with the following:‎

- A right of access to personal information held by an organization, subject to limited ‎exceptions;
- A right to correct inaccuracies in/update their personal information records; and‎
- A right to withdraw consent to the use or communication of personal information.

In addition to these rights, the Quebec Private Sector Act, as modified by Bill 64, gives individuals the right to have their personal information deindexed. A right to data portability will be coming into force on September 22, 2024.

Finally, organizations must have policies and practices in place that give effect to the ‎requirements of the legislation and organizations must ensure that their employees are ‎made aware of and trained with respect to such policies.‎

TRANSFER

When an organization transfers personal information to a third-party service provider (*ie*, ‎who acts on behalf of the transferring organization -- although Canadian legislation does not use these terms, the transferring organization would be the “controller” in GDPR parlance, and the service provider would be a “processor”), the transferring organization ‎remains accountable for the protection of that personal information and ensuring ‎compliance with the applicable legislation, using contractual or other means. In particular, the transferring organization is ‎responsible for ensuring (again, using contractual or other means) that the third party service provider appropriately safeguards ‎the data, and would also be required under the notice and openness/transparency ‎provisions to reference the use of third-party service providers in and outside of Canada ‎in their privacy policies and procedures.‎

These concepts apply whether the party receiving the personal information is inside or outside Canada. Transferring personal information outside of Canada for storage or processing is generally permitted so long as the requirements discussed above are addressed, and the transferring party notifies individuals that their information may be transferred outside of Canada and may be subject to access by foreign governments, courts, law enforcement or regulatory agencies. This notice is typically provided through the transferring party’s privacy policies.

With respect to the use of foreign service providers, PIPA Alberta specifically requires a ‎transferring organization to include the following information in its privacy policies and ‎procedures:‎

- The countries outside Canada in which the collection, use, disclosure or storage is ‎occurring or may occur, and
- The purposes for which the third party service provider outside Canada has been ‎authorized to collect, use or disclose personal information for or on behalf of the ‎organization

Under PIPA Alberta, specific notice must also be provided at the time of collection or ‎transfer of the personal information and must specify:‎

- The way in which the individual may obtain access to written information about the ‎organization’s policies and practices with respect to service providers outside ‎Canada, and

- The name or position name or title of a person who is able to answer on behalf of ‎the organization the individual’s questions about the collection, use, disclosure or ‎storage of personal information by service providers outside Canada for or on ‎behalf of the organization.‎

The Quebec Private Sector Act, as modified by Bill 64, requires all organizations to inform persons that their personal information may be transferred outside of Québec: this is typically done at the time the information is collected. Additionally, before transferring personal information outside of the province of Quebec, organizations conduct data privacy assessments and enact ‎appropriate ‎contractual safeguards to ensure that the information will benefit from adequate protection in the jurisdiction of transfer. These assessments must take into account the sensitivity of the information, the purposes, the level of protection (contractual or otherwise) and the applicable privacy regime of the jurisdiction of transfer. Cross-border transfers may only occur if the organization is satisfied that the information would receive an adequate level of protection. Quebec has decided not to implement a system of ‎adequacy decisions, and ‎therefore assessments are required prior to any ‎cross-jurisdiction transfer.

SECURITY

Each of the Canadian Privacy Statutes contains safeguarding provisions designed to protect personal information. In essence, these provisions require organizations to take reasonable technical, physical and administrative measures to protect personal information against loss or theft, unauthorized access, disclosure, copying, use, modification or destruction. These laws do not generally mandate specific technical requirements for the safeguarding of personal information.

BREACH NOTIFICATION

Currently, PIPEDA, PIPA Alberta, and the Quebec Private Sector Act are the only Canadian Privacy Statutes ‎with breach notification requirements.‎

In Alberta, an organization having personal information under its control must, without ‎unreasonable delay, provide notice to the Commissioner of any incident involving the ‎loss of or unauthorized access to or disclosure of personal information where a ‎reasonable person would consider that there exists a real risk of significant harm to an ‎ individual as a result.‎

Notification to the Commissioner must be in writing and include:‎

- A description of the circumstances of the loss or unauthorized access or disclosure
- The date or time period during which the loss or unauthorized access or disclosure ‎occurred
- A description of the personal information involved in the loss or unauthorized access ‎or disclosure
- An assessment of the risk of harm to individuals as a result of the loss or ‎unauthorized access or disclosure
- An estimate of the number of individuals to whom there is a real risk of significant ‎harm as a result of the loss or unauthorized access or disclosure
- A description of any steps the organization has taken to reduce the risk of harm to ‎individuals
- A description of any steps the organization has taken to notify individuals of the loss ‎or unauthorized access or disclosure, and
- The name and contact information for a person who can answer, on behalf of the ‎organization, the Commissioner’s questions about the loss of unauthorized ‎access or disclosure

Where an organization suffers a loss of or unauthorized access to or disclosure of ‎personal information as to which the organization is required to provide notice to the ‎Commissioner, the Commissioner may require the organization to notify the individuals ‎to whom there is a real risk of significant harm. This notification must be given directly ‎to the individual (unless specified otherwise by the Commissioner) and include:‎

- A description of the circumstances of the loss or unauthorized access or disclosure
- The date on which or time period during which the loss or unauthorized access or ‎disclosure occurred
- A description of the personal information involved in the loss or unauthorized access ‎or disclosure
- A description of any steps the organization has taken to reduce the risk of harm, ‎and

- Contact information for a person who can answer, on behalf of the organization, ‎questions about the loss or unauthorized access or disclosure

The breach notification provisions under PIPEDA are very similar to the breach ‎notification provisions under PIPA Alberta. The main difference is that PIPEDA requires organizations to notify both the affected individuals and the federal regulator if the breach creates a real risk of significant harm to the individuals (whereas PIPA Alberta requires the initial notice only to the regulator, and then to the individuals if the regulator requires it. In practice, many organizations notify affected Albertans regardless of whether the Alberta Commissioner requires (and the Commissioner typically does require it for most reported breaches in any event). Further, under PIPEDA, organizations must also ‎keep a record of ALL information security breaches, even those which do not meet the ‎risk threshold of a “real risk of significant harm.”‎

The Quebec Private Sector Act, as modified by Bill 64, introduced a number of new obligations in ‎connection with “confidentiality incidents”, which are defined as unauthorized access, use, or communication of personal ‎ information, or the loss of such information, which were previously absent in Quebec privacy law‎. These include:‎

- A general obligation to ‎prevent, mitigate and remedy security incidents
- The obligation to notify the CAI and the person affected ‎whenever the incident presents a risk of ‎ ‎“serious ‎injury.” Factors to consider when evaluating the ‎risk of serious injury include the sensitivity of the ‎information ‎concerned, the anticipated consequences of the ‎use of the information and the likelihood ‎that the information will ‎be used for harmful purposes. Although the Quebec Private Sector Act requires organizations to act “promptly” and “with diligence” in response to confidentiality breaches, it does not provide specific timeframes within which such notifications must be made, and
- The obligation on to keep a register of confidentiality ‎incidents, with the CAI having extensive audit rights

Quebec recently adopted regulations further detailing the reporting, notification, and record-keeping obligations of organizations in connection with confidentiality incidents.

ENFORCEMENT

Canadian privacy regulatory authorities have an obligation to investigate complaints, as well as the authority to initiate complaints.

Under PIPEDA, a complaint must be investigated by the Commissioner and a report will be prepared that includes the Commissioner’s findings and recommendations. A complainant (but not the organization subject to the complaint) may apply to the Federal Court for a review of the findings and the court has authority to, among other things, order an organization to correct its practices and award damages to the complainant, including damages for any humiliation that the complainant has suffered.

Under PIPA Alberta and PIPA BC, an investigation may be elevated to a formal inquiry by the Commissioner resulting in an order. Organizations are required to comply with the order within a prescribed time period, or apply for judicial review. In both BC and Alberta, once an order is final, an affected individual has a cause of action against the organization for damages for loss or injury that the individual has suffered as a result of the breach.

In Alberta and BC, a person that commits an offence may be subject to a fine of not more than CA$100,000. Offences include, among other things, collecting, using and disclosing personal information in contravention of the Act (in Alberta only), disposing of personal information to evade an access request, obstructing the commissioner, and failing to comply with an order.

Similarly, under the Quebec Private Sector Act, an order from the CAI must be complied with within a prescribed time period. An individual may appeal to the judge of the Court of Quebec on questions of law or jurisdiction with respect to a final decision.

The Quebec Private Sector Act, as modified by Bill 64, introduced a regime of steep fines and administrative penalties in case of non-compliance. The maximum penalties range between CA$5,000 and CA$100,000 in the case of individuals, and up to between CA$15,000$ and CA$25 million or 4% of worldwide turnover for the preceding fiscal year for organizations. This new penalty regime represents a significant change with the previous Quebec regime, under which the maximum penalties were limited to CA $20,000.

There are also statutory privacy torts in various provinces under separate legislation, and Ontario courts have recognized a common-law cause of action for certain privacy torts. In Quebec, a general right to privacy also exists under the *Civil Code of Quebec* and the *Charter of Human Rights and Freedoms*. Organizations may face litigation (including class action litigation) under these statutory and common-law torts, as well as under the general regime of civil liability in Quebec, in addition to any enforcement or claims under Canadian Privacy Statutes.

ELECTRONIC MARKETING

Electronic marketing is governed by both Canadian Privacy Statutes (as discussed ‎above), as well as Canada’s Anti-Spam Legislation (CASL).‎

CASL is a federal statute which prohibits sending, or causing or permitting to be sent, a commercial electronic message (defined broadly to include text, sound, voice, or image messages aimed at encouraging participation in a commercial activity) unless the recipient has provided express or implied consent and the message complies with the prescribed content and unsubscribe requirements (subject to limited exceptions).

What constitutes both permissible express and implied consent is defined in CASL and its regulations. For example, an organization may be able to rely on implied consent when there is an “existing business relationship” with the recipient of the message, based on:

- A purchase by the recipient within the past two years, or
- A contract between the organization and the recipient currently in existence or which ‎expired within the past two years

CASL also prohibits the installation of a computer program on any other person's ‎computer system, or having installed such a computer program to cause any electronic ‎messages to be sent from that computer system, without express consent, if the ‎relevant system or sender is located in Canada. In addition, the Act contains anti ‎phishing provisions that prohibit (without express consent) the alteration of transmission ‎data in an electronic message such that the message is delivered to a destination other ‎than (or in addition to) that specified by the sender.‎

CASL also introduced amendments to PIPEDA that restrict 'address harvesting', or the ‎unauthorized collection of email addresses through automated means (i.e., using a ‎computer program designed to generate or search for, and collect, email addresses) ‎without consent. The use of an individual’s email address collected through address ‎ harvesting also is restricted.‎

The 'Competition Act' was also amended to make it an offence to provide false or ‎misleading representations in the sender information, subject matter information, or ‎content of an electronic message.‎

CASL contains potentially stiff penalties, including administrative penalties of up to ‎CA$1 million per violation for individuals and CA$10 million for corporations (subject to a ‎due diligence defense). CASL also sets forth a private right of action permitting ‎individuals to bring a civil action for alleged violations of CASL (CA$200 for each ‎contravention up to a maximum of CA$1 million each day for a violation of the ‎provisions addressing unsolicited electronic messages). However, the private right of ‎action is not yet in force, and there is currently little expectation that it will ever come into force.‎

ONLINE PRIVACY

Online privacy is governed by Canadian Privacy Statutes (discussed above). In ‎general, Canadian privacy regulatory authorities have been active in addressing online ‎privacy concerns.‎

For example, in the context of social media, the OPC has released numerous Reports ‎of Findings addressing issues including:‎

- Default privacy settings
- Social plug-ins

- Identity authentication practices, including data scraping and voiceprint
- The collection, use and disclosure of personal information on social networking sites, including for marketing purposes‎
- The OPC has also released decisions and guidance on privacy in the context of ‎Mobile Apps

In addition, the OPC has released findings and guidelines related to the use of cookies ‎and online behavioral advertising, including findings indicating that information stored by ‎temporary and persistent cookies is considered to be personal information and ‎therefore subject to PIPEDA. The OPC has adopted the same position with respect to ‎ information collected in connection with online behavioral advertising.‎

In ‘Privacy and Online Behavioral Advertising’, the OPC stated that it may be permissible to use opt-out consent in the context of online behavioral advertising if the following conditions are met:‎

- Individuals are made aware of the purposes for the online behavioral advertising, at ‎or before the time of collection, in a manner that is clear and understandable
- Individuals are informed of the various parties involved in the online behavioral ‎advertising at or before the time of collection
- Individuals are able to opt-out of the practice and the opt-out takes effect ‎immediately and is persistent
- The information collected is non-sensitive in nature (*ie*, not health or financial ‎information), and
- The information is destroyed or made de-identifiable as soon as possible

The OPC has indicated that online behavioral advertising must not be a condition of ‎service and, as a best practice, should not be used on websites directed at children.‎

Canadian privacy regulatory authorities also consider location data, whether tied to a static location or a mobile device, to be personal information. As such, any collection, use or disclosure of location data requires, among other things, appropriate notice, and consent. Most of the privacy regulatory authority decisions related to location data have arisen with respect to the use of GPS in the employment context.

The Canadian privacy regulatory authorities provide the following test that must be met ‎for the collection of GPS data (and other types of monitoring and surveillance activities):‎

- Is the data demonstrably necessary to meet a specific need?‎
- Will the data likely be effective in meeting that need?‎
- Is the loss of privacy proportional to the benefit gained? ‎
- Are there less privacy-intrusive alternatives to achieve the same objective?‎

Bill 64 introduced several changes to the Quebec Private Sector Act which significantly impact online privacy. Starting September 22, 2023, organizations collecting personal information by offering a product or service with privacy parameters must ensure that the highest privacy settings are enabled by default. Additionally, organizations collecting personal information from persons using tracking, localization or profiling technology (including cookies, trackers, and similar technologies) have the obligation to inform the person in advance of the use of such technologies, and to inform the person of the method for activating such functions: the use of such technologies therefore requires opt-in consent. “Profiling” is broadly defined as the collection and use of personal information in order to evaluate certain characteristics of a person such as workplace performance, economic or financial situation, health, personal preferences or interest, or behaviour.

Artificial Intelligence

The OPC has also issued guidance on the appropriate use of generative AI systems and has stated that generative AI systems should be developed with the general principles of legality, appropriate purposes, necessity and proportionality, openness and accountability, and:

- In a manner that allows individuals to meaningfully exercise their rights to access their personal information; while
- limiting collection, use and disclosure to only what is needed to fulfill the identified purpose; and
- implementing appropriate safeguards

In addition, the OPC has stated that developers of generative AI models should take steps to ensure that outputs should be as accurate as possible.

KEY CONTACTS

Tamara Nielsen
Counsel
T +1 604.643.2952
tamara.nielsen@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CAPE VERDE

Last modified 8 January 2022

LAW

Data Protection Law (Law 133/V/2001 (as amended by Law 41/VIII/2013, Law 121/IX/2021 of 17 March 2021) and Law 132/V /2001, of 22 January 2001.

DEFINITIONS

Definition of personal data

Personal data is defined as any information, regardless of its nature or the media on which it is stored, relating to an identifiable natural person (referred to as 'the data subject'). Natural persons are deemed to be identifiable whenever they can be directly or indirectly identified through such information.

Definition of sensitive personal data

Sensitive data is defined as personal data that refers to a person’s:

- philosophical or political convictions
- party or union affiliation
- religious faith
- private life
- ethnic origin
- health
- sex life
- genetic information and biometric data.

NATIONAL DATA PROTECTION AUTHORITY

The national data protection authority in Cape Verde is the *Comissão Nacional de Proteção de Dados Pessoais* ('data protection authority').

REGISTRATION

Pursuant to the Data Protection Law, before starting the processing of personal data (and considering the specific categories of personal data), prior authorization or registration with the data protection authority is required.

Specific prior written registration (ie authorization) granted by the data protection authority is necessary in the following cases:

- the processing of sensitive data (except in certain specific cases eg if the processing relates to data which is manifestly made public by the data subject, provided his consent for such processing can be clearly inferred from his/her statements) and only in cases where the data subject has given his/her consent to the use of such data
- the processing of data in relation to creditworthiness or solvency
- the interconnection of personal data
- the use of personal data for purposes other than those for which it was initially collected.

DATA PROTECTION OFFICERS

The appointment of a data protection officer is mandatory when:

- processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 8 (sensitive data) or personal data relating to criminal convictions and offences referred to in Article 11 (criminal convictions and offences).

COLLECTION & PROCESSING

The collection and processing of personal data is subject to the rules laid down in the Data Protection Law. As a general note, personal data processing operations may only be undertaken once one of the following requirements are met:

- lawfulness;
- consent;
- performance of a contract;
- legitimate interests, public interests, vital interests of data subject or legal duty.

Moreover, as previously stated, there are some cases (referred to above) in which the collection and processing of personal data is subject to prior authorization from the data protection authority.

TRANSFER

The Data Protection Law stipulates that the international transfer of personal data is only permitted if the recipient country is considered to have a sufficient level of protection in respect of personal data processing.

The sufficient level of protection for foreign countries is defined by the data protection authority.

As a general rule, the transfer of personal data to countries that do not provide for an adequate level of protection of personal data can only be permitted if the data subject has given his consent or in some specific situations, namely if the transfer:

- is necessary for the performance of an agreement between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject’s request
- is necessary for the performance or execution of a contract entered into or to be entered into in the interest of the data subject between the controller and a third party
- is necessary in order to protect the vital interests of the data subject
- is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, provided the conditions laid down in law for consultation are fulfilled in the particular case.

SECURITY

The Cape Verdean Data Protection Law stipulates that data controllers must implement technical and organizational measures so as to ensure the confidentiality and security of the personal data processed. Such obligations must also be contractually enforced by the data controller against the data processor. Moreover, certain specific security measures must be adopted regarding certain types of personal data and purposes (notably, sensitive data, call recording, video surveillance etc.).

BREACH NOTIFICATION

There a duty to notify CNPD in case of a data breach no later than 72 hours after becoming aware of the same, unless it is considered that such breach does not pose a risk to the rights, freedoms and warranties of the data subjects.

ENFORCEMENT

Enforcement of the Data Protection Law is done by the data protection authority – CNPD.

Moreover, the Data Protection Law sets out criminal and civil liability as well as additional sanctions for breaches of the provisions of said statute.

Civil Liability

Any person who has suffered pecuniary or non-pecuniary loss as a result of any inappropriate use of personal data has the right to bring a civil claim against the relevant party. Criminal Liability The DPL provides that all of the following constitute criminal offences:

- a failure to notify or to obtain the authorization of the DPA prior to commencing data processing operations that require such authorization
- provision of false information in requests for authorization or notification
- misuse of personal data (ie processing personal data for different purposes than those for which the notification / authorization was granted)
- the interconnection of personal data without the authorization of the DPA
- unlawful access to personal data
- a failure to comply with a request to stop processing personal data.

These offences are punishable with a term of imprisonment of up to 2 years or a fine of up to 240 days.

Additional Sanctions

The DPL also lays down sanctions that can be imposed in addition to criminal and civil liability, namely:

- a temporary or permanent prohibition on processing data
- the advertisement of a sentence applied to a specific case
- a public warning or reproach of a data controller.

ELECTRONIC MARKETING

Law 132/V/2001 provides an opt-in right for direct marketing communications. Moreover, both Law 132/V/2001 and the Data Protection Law grant data subjects the right to object to unsolicited communications, at his/her request and free of any costs, to any data processing in relation to marketing activities.

ONLINE PRIVACY

Law 132/V/2001 lays down the legal framework for data protection in the telecommunications sector. Special rules include the following:

- any personal data obtained through phone calls performed by public operators or telecommunication public service providers must be erased or made anonymous after the phone call has ended
- traffic data can only be processed for billing, customer information or support, fraud prevention and the selling of telecommunication services.

KEY CONTACTS

Costa Cunha Gonçalves & Associados
www.mirandalawfirm.com/

António Gonçalves
Partner
Costa Cunha Gonçalves & Associados
antonio.goncalves@ccg.cv

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CAYMAN ISLANDS

Last modified 26 January 2023

LAW

The Data Protection Act (2021 revision) (**DPA**) is a Cayman Islands law, which first came into force on 30 September 2019. The DPA introduced the first legislative framework on data protection in the Cayman Islands.

Application

The application of the DPA turns on whether an organization is established in the Cayman Islands or has personal data processed in the Cayman Islands. Specifically, the DPA applies to a data controller in respect of personal data only if:

- the data controller is established in the Cayman Islands and the personal data are processed in the context of that establishment; or
- the data controller is not established in the Cayman Islands, but the personal data are processed in the Cayman Islands other than for the purposes of transit of the data through the Cayman Islands.

For these purposes, '*established in the Cayman Islands*' means:

- a body incorporated, or a partnership or other unincorporated association formed, under the laws of the Cayman Islands;
- a body registered as a foreign company under the laws of the Cayman Islands;
- an individual who is ordinarily resident in the Cayman Islands; or
- any other person who maintains (i) an office, branch or agency in the Cayman Islands through which the person carries on any activity; or (ii) a regular practice in the Cayman Islands.

A data controller not established in the Cayman Islands that processes personal data in the Cayman Islands is required to appoint a local representative established in the Cayman Islands who, for all purposes within the Cayman Islands, is the data controller and bears all obligations under the DPA as if it were the data controller.

DEFINITIONS

The DPA defines '**personal data**' as data relating to a living individual who can be identified, including data such as:

- the living individual's location data or online identifier;
- factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the living individual;
- an expression of opinion about the living individual; and
- any indications of the intentions of the data controller or any other person in respect of the living individual.

The DPA creates more restrictive rules for the processing of '**sensitive personal data**', which includes personal data consisting of a data subject's racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, physical or mental health or condition, medical data, sex life or commission or alleged commission of an offence or related proceedings.

Under the DPA the '**processing**' of personal data has an extremely broad meaning and includes obtaining, recording or holding data, or carrying out any operation on personal data.

Personal data may be processed by either a **data controller** or a **data processor**. The data controller is the decision maker, the person who '*alone or jointly with others determines the purposes, conditions and manner in which any personal data are, or are to be, processed*'. The data processor '*processes personal data on behalf of a data controller*'. The obligations under the DPA are imposed almost exclusively on the data controller.

A '**data subject**' is an identified living individual or a living individual who can be identified directly or indirectly by means reasonably likely to be used by the data controller or by any other person.

NATIONAL DATA PROTECTION AUTHORITY

The supervisory authority under the DPA is the Office of the Ombudsman of the Cayman Islands (the **Ombudsman**), who periodically issues detailed guidance on the DPA, most recently in May 2023, accessible on the Ombudsman's website at https://ombudsman.ky/data-protection.

The Ombudsman's contact details are as follows:

Office of the Ombudsman

PO Box 2252

Grand Cayman KY1-1107

CAYMAN ISLANDS

Email: info@ombudsman.ky

Telephone number: +1 345 946 6283

REGISTRATION

There is currently no requirement for a data controller or data processor to notify the Ombudsman of their role or complete any registration.

DATA PROTECTION OFFICERS

There is no requirement for organizations to appoint a data protection officer under the DPA, though this may be recommended for larger or complex organizations.

COLLECTION & PROCESSING

A data controller is responsible for compliance with a set of eight core principles which apply to the personal data that the data controller processes. A data controller is also responsible for ensuring that the principles are complied with in relation to personal data processed on the data controller's behalf.

Under these principles:

- Personal data must be processed fairly, lawfully and in a transparent manner;
- Personal data must be obtained for specified lawful purposes and not further processed in any manner incompatible with those purposes;
- Personal data must be adequate, relevant and not excessive in relation to the purposes;
- Personal data must be accurate and where necessary kept up-to-date;
- Personal data must not be kept for longer than is necessary for the purposes it was collected for;
- Personal data must be processed in accordance with the rights of data subjects under the DPA;

- Appropriate technical and organizational measures must be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; and
- Personal data must not be transferred to a country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

For purposes of the first principle (fair and lawful processing), personal data will not be treated as processed fairly unless the data subject has, as soon as reasonably practicable, been provided with, at a minimum, the identity of the data controller and the purpose for which the data are to be processed. This is usually communicated in the form of a privacy notice.

In order for the processing to be considered lawful, the processing must be justified by reference to an appropriate basis. The legal bases (also known as lawful grounds) for processing personal data are:

- The data subject has given consent to the processing (where consent must be freely given, specific, informed and unambiguous and must be capable of being withdrawn at any time);
- The processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject with a view to entering into a contract;
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject;
- The processing is necessary for the administration of justice or the exercise of a function by a public authority or conferred under law or other function of a public nature exercised in the public interest; and
- The processing is necessary for the purposes of legitimate interests pursued by the data controller or a third party to whom the data is disclosed, except if the processing is unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Sensitive personal data

In order for the processing of sensitive personal data to be considered lawful, in addition to meeting one of the above legal bases, one of the following conditions must be met:

- The data subject has given consent to the processing (where consent must be freely given, specific, informed and unambiguous and must be capable of being withdrawn at any time);
- The processing is necessary for the purposes of exercising or performing a right or obligation conferred or imposed by law on the data controller in connection with the data subject's employment;
- The processing is necessary to protect the vital interests (i) of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject; or (ii) of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;
- The processing is carried out by a not-for-profit body in certain limited circumstances;
- The information contained in the personal data has been made public as result of steps taken by the data subject;
- The processing is necessary for the purposes of legal proceedings, obtaining legal advice or otherwise establishing, exercising or defending legal rights;
- The processing is necessary for the administration of justice or the exercise of a function by a public authority or conferred under law; or
- The processing is necessary for medical purposes and is undertaken by a health professional or person who owes an equivalent duty of confidentiality.

Rights of the Data Subject

Right of access

Upon written request, a data subject is entitled to be informed by a data controller of whether their personal data are being processed by or on behalf of the data controller and, if so, to be given a description of such personal data together with prescribed information about how the data have been used by the data controller. A data subject is also entitled, upon written request, to a copy of their personal data and any information available as to the source of such personal data. A data controller is generally required to comply with such a request within 30 days.

Right to object to processing

A data subject is entitled, at any time by notice in writing, to require a data controller to cease processing, or not to begin processing, or to cease processing for a specified purpose or in a specified manner, the data subject's personal data. A data controller is required to comply with such a notice as soon as practicable and in any case within 21 days, unless the processing is necessary:

- for the performance of a contract to which the data subject is a party or the taking of steps at the request of the data subject with a view to entering into a contract;
- for compliance with a legal obligation to which the data controller is subject; or
- in order to protect the vital interests of the data subject.

In addition, data subjects have an unconditional right to require a data controller at any time to cease (or not to begin) processing their personal data for the purposes of direct marketing.

Rights in relation to automated decision-making

A data subject is entitled, at any time by notice in writing, to require a data controller to ensure that no decision taken by or on behalf of the data controller that significantly affects the data subject is based solely on the processing by automatic means of the data subject's personal data for the purpose of evaluating the data subject's performance at work, creditworthiness, reliability, conduct or any other matters relating to the data subject.

Where a decision that significantly affects a data subject is based solely on processing by automatic means, subject to certain exceptions, the data controller is required as soon as reasonably practicable to notify the data subject that the decision was taken on that basis, and the data subject is then entitled to require the data controller to reconsider the decision.

Right to rectification

The DPA includes an indirect right for individuals to have inaccurate personal data rectified, by making such a request to the data controller. There is no explicit obligation for a data controller to act on such a request, however data controllers are generally required under the principles to process data fairly and transparently and ensure that personal data is accurate and kept up-to-date.

Any person may make a complaint to the Ombudsman about the processing of personal data and the Ombudsman may order the data controller (among other things) to rectify, block, erase or destroy the relevant data.

TRANSFER

As set out in the eighth principle, transfers of personal data by a data controller or a data processor to countries or territories outside the Cayman Islands are only permitted where that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. This is to ensure that the level of protection provided by the DPA is not circumvented by transferring personal data abroad.

The Ombudsman has issued guidance stating that it considers the following countries and territories as ensuring an adequate level of protection:

- member states of the European Economic Area (that is, the European Union plus Lichtenstein, Norway and Iceland) where Regulation EU 2016/679 (the General Data Protection Regulation or "GDPR") is applicable; and
- any country or territory in respect of which an adequacy decision has been adopted by the European Commission pursuant to Article 45(3) GDPR or remains in force pursuant to Article 45(9) of the GDPR.

Other countries and territories may be deemed to have an adequate level of protection depending on various factors, which are to be assessed by a data controller, or a data controller may request authorization from the Ombudsman for a transfer.

The DPA also includes the following exceptions where the eighth principle will not apply to a transfer:

- if the data subject has consented to the transfer (where consent must be freely given, specific, informed and unambiguous and must be capable of being withdrawn at any time);
- where the transfer is necessary for the performance of a contract between the data subject and the data controller, or the taking of steps at the request of the data subject with a view to the data subject's entering into a contract with the data controller;
- the transfer is necessary for the conclusion of a contract between the data controller and a person other than the data subject, being a contract that is entered into at the request of the data subject, or is in the interests of the data subject, or for the performance of such a contract;
- the transfer is necessary for reasons of substantial public interest;
- the transfer is necessary for the purposes of legal proceedings, obtaining legal advice or otherwise establishing, exercising or defending legal rights;
- the transfer is necessary in order to protect the vital interests of the data subject;
- the transfer is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by a person to whom the data are or may be disclosed after the transfer; or
- the transfer is required under international cooperation arrangements between intelligence agencies or between regulatory agencies to combat organized crime, terrorism or drug trafficking or to carry out other cooperative functions, to the extent permitted or required under Cayman Islands law or an order of the Grand Court of the Cayman Islands.

SECURITY

The DPA is not prescriptive about specific technical standards or measures that must be taken to protect personal data. Rather, the DPA adopts a context-specific approach, requiring that appropriate technical and organization measures be taken, appropriate to the risks presented by the processing. A data controller should take into account the state of the art, costs of implementation, as well as the nature, scope, context and purpose of their processing.

Aspects to consider include:

- organizational measures, e.g. staff training and policy development;
- technical measures, e.g. physical protection of data, pseudonymization, encryption; and
- securing ongoing availability, integrity and accessibility, e.g. by ensuring backups.

BREACH NOTIFICATION

The DPA contains a general requirement for a personal data breach to be notified by the data controller to the Ombudsman and the relevant data subject(s). A personal data breach is a wide concept, defined as '*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed*'.

The data controller must notify a breach to the relevant data subject(s) and the Ombudsman without undue delay, and in any case no longer than five days after the data controller should, with the exercise of reasonable diligence, have been aware of the breach.

The same rules apply where a breach occurs at the level of a data processor. Accordingly, data controllers should contractually require their data processors to notify the data controller of a breach in a timely manner.

The notification must describe the nature of the breach, the consequences of the breach, the measures proposed to be taken by the data controller to address the breach and the measures recommended by the data controller to the relevant data subject(s) to mitigate the possible adverse effects of the breach.

ENFORCEMENT

A breach of the DPA constitutes a criminal offence, punishable on conviction to a fine of up to CI$100,000 (approx. US$125,000), imprisonment for a term of up to 5 years, or both.

In addition, the DPA empowers the Ombudsman to issue monetary penalty orders of up to CI$250,000 (approx. US$300,000) where the Ombudsman is satisfied on a balance of probabilities that there has been a serious contravention of the law by a data controller and the contravention was of a kind likely to cause substantial damage or substantial distress to a data subject.

Investigative and corrective powers

The Ombudsman is given wide investigative and corrective powers under the DPA, including to require the provision of information and to issue orders to carry out specific remediation activities.

Right to claim compensation

The DPA specifically provides for individuals to bring private claims against data controllers: any person who suffers damage by reason of a contravention by a data controller of any requirement of the DPA has a cause of action for compensation from the data controller for that damage.

Personal liability

The DPA explicitly provides for personal liability for offences committed by a body corporate where the offence is proven to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, any director, secretary or similar officer or any person purporting to act in such capacity. Where the affairs of a body corporate are managed by its members, this personal liability also applies to the acts and defaults of a member in connection with the member's functions of management.

ELECTRONIC MARKETING

The DPA applies to most electronic marketing activities as these will involve some use of personal data (e.g., an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent or the legitimate interests of the data controller. Where consent is relied upon, the strict standards for consent under the DPA are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to require a data controller at any time to cease (or not to begin) processing their personal data for the purposes of direct marketing (which includes direct electronic marketing).

ONLINE PRIVACY

There are no specific restrictions addressing online privacy beyond those generally applicable to the processing of personal data under the DPA. Personal data explicitly includes online identifiers.

KEY CONTACTS

Carey Olsen
www.careyolsen.com

Nick Bullmore
Partner
T +1 345 749 2000
nick.bullmore@careyolsen.com

Graham Stoute
Counsel
Carey Olsen
T +1 345 749 2014
graham.stoute@careyolsen.com

Jenna Willis
Counsel
Carey Olsen

T +1 345 749 2053
jenna.willis@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CHAD

Last modified 17 January 2024

LAW

The data protection regime in Chad is mainly governed by the following laws and regulations:

- Act No. 007/PR/2015 of February 10, 2015, on Personal Data protection (‘**The Act**’);
- Decree No. 075/PR/2019 of January 21, 2019 implementing the provisions of application of the Act N°007/PR/2015 of February 10, 2015 on the protection of personal data;
- Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification;
- Ordinance No. 002/PR/2019 amending Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification;
- Ordinance No.012/PT/2023 dated 1st August 2023 amending the Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification;
- Ordinance No. 014/PT/2023 dated 30 August 2023 amending the Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification;
- Ordinance No. 009/PCMT/2022 amending Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification;
- Act No. 009/PR/2015 on the cybersecurity and the fight against the cybercrime;
- Ordinance No. 008/PCMT/2022 on the Cybersecurity in the Republic of Chad; and
- Act No. 008/PR/2015 on electronic transactions.

DEFINITIONS

Definition of Personal Data

Personal data: Any information relating to a natural person, identified or identifiable directly or indirectly, by reference to an identification number or to one or more elements specific to his or her physical, physiological, genetic, psychological, cultural, social, and economic identity. (Article 5 of the Act)

Definition of Sensitive Personal Data

Sensitive data: Data relating to religious, philosophical, political, trade union opinions or activities, sex or racial life, health, social measures, prosecutions, and criminal or administrative charges. (Article 5 of the Act)

NATIONAL DATA PROTECTION AUTHORITY

The National Data Protection Authority is the *Agence Nationale de Sécurité Informatique et de Certification É lectronique* ('**ANSICE**').

ANSICE is responsible for ensuring compliance, on the national territory, with the provisions of the Act. As such, it has the power to sanction any violation of the Act.

ANSICE main duties include:

- informing the data holders and the data controllers of their rights and obligations;
- receiving the formalities prior to the creation of processing of personal data;
- receiving complaints, petitions and claims relating to the implementation of the processing of personal data and informs their authors of the follow-up given to them;
- informing the judicial authorities without delay of the offences of which it has knowledge;
- entitling its members or agents with the task of carrying out verifications relating to any processing and, where appropriate, obtaining copies of any document or information medium useful for its mission;
- imposing a sanction on a data controller;
- keeping a directory of personal data processing at the disposal of the public;
- authorizing, under the conditions provided for in the Act, the transborder transfer of personal data.

(Article 6 of the Act Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification)

REGISTRATION

The is no country-wide system of registration in Chad. However, the processing of personal data may be subject to prior notification to, or authorization/Prior approval from the CDP.

Regime of authorisation

The authorisation of the ANSICE is required for the processing of any personal data relating to:

- genetic, biometric data, and research in the health field;
- offenses, convictions, or security measures;
- interconnection of files;
- national identification number or any other identifier of the same nature; or
- public interest in particular for historical, statistical, or scientific purposes.

The regime of declaration

Apart from the data provided for by the authorisation regime, any processing of personal data must be declared in a written form and addressed to ANSICE.

Notice/Opinion regime ("Avis")

The automated processing of personal information carried out on behalf of the State, a public institution or a local authority or a legal person under private law managing a public service are decided by regulatory act taken after a reasoned opinion from the ANSICE. Such processing relates to:

1. State security, defense or public safety;
2. the prevention, investigation, recording or prosecution of criminal offences or the execution of criminal sentences or security measures;
3. the population census;
4. personal data that reveal, directly or indirectly, the racial, ethnic or regional origins, parentage, political, philosophical or religious opinions or trade union membership of persons, or that relate to the health or sexual life of persons when they are not covered by provisions related to interconnexion of data;
5. the processing of salaries, pensions, taxes, and other settlements.

(Articles 51, 52 and 53 of the Act)

DATA PROTECTION OFFICERS

There are no specific provisions relating to the appointment of a Data Protection Officers (‘**DPO**’) under the Act. This issue is left at the exclusive discretion of the data controllers.

COLLECTION & PROCESSING

Data collection and processing are subject to the following principles and requirements:

- The collection, recording, processing, storage, and transmission of personal data must be lawful, fair, and not fraudulent;
- Data must be collected for specified, explicit, and legitimate purposes;
- Data must be relevant and not excessive in relation to the purposes for which they are collected and further processed;
- Data must be kept for a period not exceeding the period necessary for the purposes for which they were collected /processed;
- The data collected must be accurate and, if necessary, updated whenever necessary;
- Data controller must inform the data subject of any personal data processing operation that involves personal data; and
- Personal data must be treated confidentially and protected.

The Data holders/subjects have rights to:

- **To be informed:** Pursuant to Article 35 and seq. of the Act, the data controller must inform the data subject of:
  - the identity of the data controller and its representative (if any);
  - the purposes of the processing;
  - the category of data concerned;
  - the recipients or categories of recipients of the data;
  - the right to object to the collection of such data;
  - the right to access the collected data and have it edited;
  - the duration of the processing; and
  - details on any intended transfer of the data.
- **To access:** Pursuant to Article 38 of the Act, data subjects have a right of access and they can obtain the following from the data controller:
  - information allowing for data subjects to be aware of and the possibly to contest the processing;
  - confirmation of whether his/her personal data forms part of the processing;
  - copy of his/her personal data as well as any available information on the origin of the data; and
  - information relating to the purposes of the processing, categories of data processed, recipients, or categories of recipients, to whom the data are disclosed, and information relating to the transfer of personal data outside the country.
- **To rectification:** In light of the provisions of Article 48 of the Act, any data subjects may require that the data controller rectifies their personal data if it is inaccurate, incomplete, unclear, or expired, or if the collection, usage, disclosure, or retention of the data is prohibited.
- **To erasure:** In light of the provisions of Article 48 of the Act, any data subjects may require that the data controller deletes their personal data if it is inaccurate, incomplete, unclear, or expired, or if the collection, usage, disclosure, or retention of the data is prohibited.
- **Right to object/opt-out:** Pursuant to Article 45 of the Act, any data subject has the right to object, with legitimate reasons, to the processing of his/her personal data. The data subject also has the right to be informed before his/her personal data is communicated or used by a third party and also to object the communication or the use of the personal data.

TRANSFER

In light of Article 29 of the Act, the data controller cannot transfer personal data to another foreign country non-member of the CEMAC/CEAC unless that country provides a sufficient level of protection for the privacy, fundamental rights, and freedoms of individuals.

Moreover, prior to any transfer of personal data abroad, the data controller must first inform the regulatory authority, ANSICE.

CEMAC is the French acronym of Economic and Monetary Community of Central Africa. CEEAC is the French acronym of the Economic Community of Central Africa States.

A transfer to a non CEMAC/CEEAC country not offering a sufficient level of protection is possible if:

- the Data Subject agrees to the transfer;
- the transfer protects the life of the Data Subjects/Holders;
- the transfer Protect the public interest;
- the transfer is necessary to the performance of an agreement between the Data Subject and the Data Processor or take precontractual measures upon the request of the Data Subject;
- If the transfer intervenes from a public register which, according to law and regulations, is focused on the public information and open to the public consultation.

The ANSICE may allow the Data controller to transfer data to a foreign country non-member of CEMAC/CEEAC if the Data controller provides sufficient protection for the Data Subject’s private life, liberties, and fundamental rights.

(Articles 30-33 of the Act)

SECURITY

Data Controllers are required to ensure the security of personal data. They must prevent the data’s alteration and damage, or access by non-authorised third parties. In this regard, Data Controllers should make sure that:

- Persons with access to the system can only access the data that they are allowed to access;
- The identity and interest of any third-party recipients of the data can be verified;
- The identity of persons who have access to the system (to view or add data) can be verified;
- Unauthorised persons cannot access the place and equipment used for the data processing;
- Unauthorised persons cannot read, copy, modify, destroy, or move data;
- All data entered onto the system are authorised;
- The data will not be read, copied, amended, or deleted without authorisation during the transport or communication of the data.
- The data are backed up with security copies;
- The data are renewed and converted to preserve them.

(Article 60 of the Act)

BREACH NOTIFICATION

Breach of the provisions of Personal Data Act including breach notification is subject to following administrative sanctions by the ANSICE:

- a warning to the data controller who does not comply with the obligations arising from the Law;
- a formal notice to put an end to the breaches concerned within the time limit which it fixes;
- penalties in accordance with the observed shortcomings;
- interruption of treatment for a maximum of three years;
- blocking for a maximum of three months of certain processed personal data; or
- temporary or permanent prohibition of processing contrary to the provisions of the Act.

(Article 8 Article 8 of Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification)

In addition, a judge can take the following sanctions in case of breach notification:

- Imprisonment from between 1-5 years;

- Fines between XAF 1 million to XAF 10 million.

(Article 438 of the Criminal Code)

Mandatory breach notification

No mandatory breach notification protocol is provided under Chadian law.

ENFORCEMENT

The ANSICE have enforcement powers including:

- Investigative powers: The ANSICE can conduct investigation to discover facts and evidences of the violation of the Act. Administrative fines for infringements of the Data Protection Act
- Non-compliance with the ANSICE instructions/decisions can lead to the following sanctions:
    - a warning;
    - an injunction to put an end to defaults within the time limit set by the ANSICE; or
    - a provisional withdrawal of the authorisation granted for a period of three months at the expiry of which the withdrawal becomes final.

In case of urgency, the ANSICE can:

- interrupt a processing for a duration that cannot exceed three months.
- lock certain kinds of data for a duration that cannot exceed three months; or
- rohibit, provisionally or definitively, data processing that does not comply with the Act.

Additionally, the Act has the power to issue a temporary or permanent ban. The ban does not require a court order.

(Article 8 of Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification and Article 81 of the Act)

ELECTRONIC MARKETING

Sending of marketing communications is forbidden on principle unless the recipient agrees to it.

Also, there are specific cases under which prior approval is not required:

- the recipient’s information was collected directly from him, in accordance with the provisions of the Act;
- the recipient is already a customer of the company, the marketing messages relate to products or services that are similar to those previously provided, and the recipient is given the possibility of objecting to all messages sent to him;
- if it clearly explained to the Data subjects where their data is collected that they have right to object, free of charge, to the processing of their Personal Data for electronic marketing;
- when the electronic marketing concerns the data of legal personals which are not constitute personal data.

(Article 49 of Act No. 008/PR/2015 on electronic transactions)

Breach of the provisions of Personal Data Act including breach of electronic marketing provisions are subject to following administrative sanctions by ANSICE:

- a warning to the data controller who does not comply with the obligations arising from the Law;
- a formal notice to put an end to the breaches concerned within the time limit which it fixes;
- penalties in accordance with the observed shortcomings;
- interruption of treatment for a maximum of three years;
- blocking for a maximum of three months of certain processed personal data; or
- temporary or permanent prohibition of processing contrary to the provisions of the Act.

In addition, a judge can take the following sanctions in case of violation of provisions of Act No. 008/PR/2015 on electronic transactions including on its provisions relating to electronic marketing:

- imprisonment from between 1-10 years;
- and fines between XAF 1 million to XAF 5 million.

(Article 168 of Act No. 008/PR/2015 on electronic transactions)

ONLINE PRIVACY

There is no specific restriction on the use of cookies under the Act. However, the ANSICE requires that the Data Subject is informed of the use of cookies and to collect his consent.

KEY CONTACTS

Geni & Kebe
www.dlapiperafrica.com/senegal

Mouhamed Kebe
Managing Partner
Geni & Kebe
T +221 76 223 63 30
mhkebe@gsklaw.sn

Mahamat Atteib
Associate
Geni & Kebe
T +221 77 737 41 74
m.atteib@gsklaw.sn

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CHILE

Last modified 28 January 2023

LAW

Protection of Personal Data is regulated under various laws in Chile.

Constitution of the Republic of Chile, Art. 19 N° 4

The Chilean constitution establishes the individual’s right to (i) respect and protection of private life, (ii) honor of the person and his/her family, and (iii) protection of his/her personal data. Any individual who, as a result of an arbitrary or illegal act or omission, suffers a “privation, disturbance or threat” to these rights may file a Constitutional Protective Action (“*Recurso de protección*”).

Law 19,628/1999 'On the protection of private life', commonly referred to as 'Personal Data Protection Law' (hereinafter, the 'PDPL')

The PDPL generally defines and regulates the processing of personal data in public and private databases and is thus the primary body of rules on the processing of personal data not governed by sectoral provisions (for example contained in the laws mentioned below).

Generally, the PDPL stipulates that personal data may only be processed if the processing is (i) permitted by law (*eg*, labor law, health care law, etc.) or (ii) based on the data subject’s prior informed, written consent. There are only a few narrow exceptions to this principle (*eg*, certain publicly accessible data, or purely internal data processing for certain purposes). In addition, the PDPL contains special regulations on the processing of personal data relating to economic, banking, and financial obligations.

The PDPL law also provides data subjects the right to access, rectify, delete, block and object to processing of personal data in certain cases.

Decree with Force of Law N° 3/19978, 'General Law of Banks'

Article 154 of this law establishes the confidentiality of an individual’s transactions with and through banks. The law distinguishes transactions covered by secrecy, which in principle are subject to an absolute prohibition of disclosure, and transactions covered by reserve, which may only be disclosed where a legitimate interest exists and if it cannot be foreseen that the knowledge of the disclosed data may cause financial damage to the customer.

Law 20,575/2012 establishing the 'purpose principle' for the processing of personal data of an economic, financial, banking or commercial nature

This law establishes several rules that apply to the processing of personal data referring to financial, economic, banking or commercial information, such as:

- Limited disclosures: Such data shall only be communicated to established commercial entities for the purpose of a commercial risk assessment in a credit granting process, and to entities that take part in this evaluation.
- Prohibition on requesting such type of data in the context of processes for personnel selection, pre-school, school or higher education admission, emergency medical care or application for public office.
- Providers of economic, financial, banking or commercial databases must have a system for recording the name of any person requesting database information, the reason, date and time of the request and the person responsible for delivering or transferring the information. Data subjects have the right to request access to their commercial information every four months and free of charge.
- Providers of the database must implement the principles of legitimacy, access and objection, data quality, purpose, proportionality, transparency, non-discrimination, use limitation and security in personal data processing, and designate a contact person for data subjects.

Law 19,223/1993 regulating certain computer crimes

This law establishes criminal sanctions for certain specific conduct related to the theft, destruction, obstruction, modification and illegal access and disclosure of information contained in data processing systems. It does not, however, refer specifically to personal data.

Law 20,584/2012 regulating the rights and duties of individuals in the context of healthcare

This law sets forth that all information contained in patient files or documentations of medical treatments are sensitive data, and establishes the obligation of healthcare professionals to maintain patient data confidential and to comply with the principle of purpose limitation. This law also includes certain specific cases in which such data can be submitted, partially or totally, to the data subject and to other individuals or entities.

Law 21521/2023 promotes competition and financial inclusion through innovation and technology in the provision of financial services, FinTech law (takes effect on February 3rd, 2023)

The law’s objective is to establish a broad framework to facilitate the provision of financial services using technology means. The law delegates regulatory authority to the Financial Market Commission ("**CMF**").

The following principles will guide the law: financial inclusion and innovation; competition promotion; financial client protection; adequate data protection; integrity and financial stability preservation; and prevention of money laundering and funding of drug trafficking and terrorism.

Bill to Create a Consolidated Debt Registry (Bulletin 14743-03)

The draft bill establishes the right to be forgotten in financial concerns where there are no valid grounds to keep people's personal financial data after its purpose has been completed.

The bill is in the first constitutional stage in the chamber of deputies, and we will be monitoring its progress over the coming year.

Bill regulating the protection and processing of personal data and creating the Agency for the Protection of Personal Data (Bulletin 11,144-07, consolidated with Bulletin 11,092-07)

This draft law aims to modernize the PDPL and adapt it to international standards. The most important stipulations are:

- the introduction of further legal bases for the processing of personal data in addition to consent (such as performance of a contract and legitimate interest), and additional requirements for processing sensitive data, depending on the category of data concerned.
- various basic principles, such as lawfulness, purpose limitation, proportionality, data quality, accountability, security, transparency and information, and confidentiality.
- regulations on international data transfers.
- information requirements.

- special obligations when using data processors.
- provisions on data protection by design and default and security measures.
- reporting obligations in the event of data breaches.
- introduction of the right to portability.
- the creation of a data protection authority with the competence to impose administrative fines.

The bill is under debate at the second constitutional stage in the chamber of deputies and conclusion of the legislative procedure is expected for this year.

Bill creating a Cybersecurity and Critical Information Infrastructure Framework Law (Bulletin 14847-06)

This law aims to create a harmonized regulatory framework for the strengthening of cybersecurity, both operational and regulatory and addresses essential service providers. It creates a governing body, which is in charge of deciding who the declared essential service providers will be. Declared essential service providers must implement certain technological, organizational, and informational security measures to prevent, report, and resolve cybersecurity events, manage risks, and contain and reduce the impact on operational continuity, confidentiality, and service integrity.

The bill is at the second constitutional stage in the senate.

DEFINITIONS

Definition of personal data

The PDPL defines **personal data** as any information concerning identified or identifiable natural persons.

Definition of sensitive data

Sensitive data are defined very broadly as personal data relating to the physical or moral characteristics of persons or to facts or circumstances of their private or intimate life, such as personal habits, racial origin, ideologies or political opinions, religious beliefs or convictions, physical or mental health conditions, and sexual life.

Definition of controller and data processing

The PDLP defines the **controller** ('responsible for the register or database') as the private individual or legal entity, or the respective public body, which is responsible for decisions related to the processing of personal data.

Data processing is defined as any operation or complex of operations or technical procedures, of automated or non-automated nature, that allow to collect, store, record, organize, elaborate, select, extract, confront, interconnect, dissociate, communicate, assign, transfer, transmit or cancel personal data, or use them in any other way.

NATIONAL DATA PROTECTION AUTHORITY

In Chile, there is no specific authority dedicated to overseeing matters related to data protection concerning processing activities performed by private persons or entities exists. Law 20,285/2008 on access to public information provides that the Transparency Council (*Consejo para la Transparencia*, the control body that ensures compliance with the aforementioned law which provides the rights to transparency and access to information of the state administration), shall ensure proper compliance with the data protection law by the organs of the state administration; however, the Transparency Council does not have powers to impose fines.

Since December 24, 2021, due to a provision in the newly adopted so-called Pro-Consumer Law (Law 21,398/2021), the consumer protection agency SERNAC has the competency to monitor compliance with the provisions of the data protection law in consumer matters. The SERNAC cannot impose fines but may initiate and participate in judicial proceedings and collective voluntary proceedings. This is the first time that private controllers’ processing of (consumer) personal data has been subject to regulatory control.

A special data protection authority is to be created by the above-mentioned legislative project (Bill that regulates the protection and processing of personal data and creates the Agency for the Protection of Personal Data (Bulletin 11,144-07, consolidated with Bulletin 11,092-07). However, as noted, there is no clear timeline for when to expect this bill to pass.

REGISTRATION

Public databases must be registered in the Civil Registry and Identification Service (*Servicio de Registro Civil e Identificación*). There is no obligation to register private databases.

DATA PROTECTION OFFICERS

The PDPL does not require the appointment of a Data Protection Officer.

COLLECTION & PROCESSING

According to the PDPL, personal data may be processed in the following cases:

- With informed, prior and written consent given by the data subject
- If authorized by legal provisions
- If the personal data comes from publicly accessible sources, and the data:
    - are of financial, banking or commercial nature, or
    - are contained in lists related to a category of persons that merely indicate background information such as the individuals´ membership in that category, his/her profession or activity, educational qualifications, address or date of birth, or
    - are required for direct response commercial communications or direct marketing or sale of goods or services

- Furthermore, personal data may be processed without the data subject’s consent if they are processed by private entities for their exclusive use, or that of their associated or affiliated entities use, for statistical, pricing or other purposes of general benefit to them. In practice, this exception is not of significant importance.

TRANSFER

Transfer of personal data is considered a processing activity, so all of the aforementioned rules are applicable, including the requirement to rely on a legal basis (usually consent). The PDPL does not provide or require any special provisions for the international transfer of personal data.

SECURITY

The PDPL does not establish specific measures that need to be adopted for the security of the personal data processed. It only stipulates that the controller is required to take care of the data with due diligence, being liable in case of damages.

All individuals involved in the processing of personal data (other than from publicly accessible sources) have to comply with confidentiality obligations, even after they end their work in this field.

BREACH NOTIFICATION

There is no obligation to report a data breach.

ENFORCEMENT

Since there is no special data protection authority in Chile, data protection violations must be challenged with a Constitutional Protective Action obased on an alleged violation of the constitutionally guaranteed right to protection of personal data, or with an action before the ordinary civil courts. In addition, the PDPL provides for a special type of action in the event that a controller fails to respond in a timely manner to a request to assert data subject rights ('*Habeas Data*').

With the entry into force of the Pro-Consumer Law (see in the section on Authority), and the competency thereby granted to the consumer protection agency SERNAC, consumers can lodge complaints alleging the violation of the data protection law to this authority. The SERNAC cannot impose fines, but may initiate and participate in judicial proceedings and collective voluntary proceedings.

ELECTRONIC MARKETING

Private entities are allowed to create and maintain databases for purposes of sending marketing and promotional emails, provided that the requirements mentioned in the 'Collection and Processing' section have been fulfilled.

However, any person may require that his/her information be deleted for such purposes, either permanently or temporarily.

The Chilean Consumer Protection Act (Law 19,496/1997 on the protection of consumer rights) defines 'advertising' as the communication that the provider of goods or services send to the public by any means, in order to inform and motivate the purchase goods or services. It also indicates that all promotional or advertising communication must indicate an expeditious way in which the recipients can request the suspension of the promotional communication (opt-out). After a consumer has exercised his opt out right, the sending of new communications is prohibited. In case of promotional or advertising communication sent by e-mail, the communication must also indicate the subject matter or theme and the identity of the sender.

ONLINE PRIVACY

There are no specific laws governing online privacy or cookies.

KEY CONTACTS

DLA Piper Chile
www.dlapiper.com/en-cl

Matías Zegers
Partner
DLA Piper Chile
T +56 2 2798 2604
mzegers@dlapiper.cl

Jorge Timmermann
Partner
DLA Piper Chile
T +56 2 2798 2608
jtimmermann@dlapiper.cl

Carla Illanes
Counsel
DLA Piper Chile
T +56 2 2798 2620
carla.illanes@dlapiper.cl

Juan Cristóbal Ríos
Associate
DLA Piper Chile
T +56 2 2798 2688
juancristobal.rios@dlapiper.cl

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CHINA

Last modified 29 April 2024

LAW

There is not a single comprehensive data protection law in the People's Republic of China (PRC). Instead, rules relating to personal information protection and data security are part of a complex framework and are found across various laws and regulations. That said, the three main pillars of the personal information protection framework in the PRC are the Personal Information Protection Law (PIPL), the Cybersecurity Law (CSL), and the Data Security Law (DSL).

On June 1, 2017, the CSL came into effect and became the first national–level law to address cybersecurity and data privacy protection. Draft Amendments to the CSL were issued on September 12, 2022, proposing enhanced liabilities for violating obligations of general network operation security, security protection of critical information infrastructure, network information security and personal information protection, etc.

The DSL came into force on September 1, 2021, and focuses on data security across a broad category of data (not just personal information).

Most significantly, the PIPL came into effect on November 1, 2021. The PIPL is the first comprehensive, national–level personal information protection law in the PRC. The PIPL does not replace — but instead enhances and clarifies — earlier personal information laws and regulations.

In addition to the PIPL, CSL and DSL, the following form the backbone of general personal information protection framework currently in the PRC:

- The Decision on Strengthening Online Information Protection, effective from December 28, 2012 (Decision);
- The Draft Regulation of Network Data Security Management, published for consultation on November 14, 2021;
- The Measures for the Security Assessment of Outbound Data Transfers, effective from September 1, 2022;
- The Measures for the Standard Contract for the Outbound Transfer of Personal Information, effective from 1 June 2023; and
- The Regulations on Facilitating and Regulating the Cross–border Data Transfers, effective from 22 March 2024.

In the past five years, there has also been an abundance of implementing regulations and guidelines (herein referred to as Guidelines) proposed, issued or revised to flesh out the essentials and concepts introduced under the personal information protection framework. These include, non–exhaustively:

- National Standard of Information Security Technology — Personal Information Security Specification (PIS Specification), as amended and effective from October 1, 2020;
- Guidelines on Internet Personal Information Security Protection, effective from April 19, 2019;
- National Standard of Information Security Technology — Guidelines on Personal Information Security Impact Assessment, effective from June 1, 2021;

- Draft National Standard of Information Security Technology — Requirements for Classification and Grading of Network Data, published for consultation on September 14, 2022;
- Practicing Guidelines for Network Security Standards — Technical Specification for Certification of Personal Information Cross-border Processing Activities (V2.0), effective from December 16, 2022;
- Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong–Hong Kong– Macao Greater Bay Area (Mainland, Hong Kong), effective from 10 December 2023;
- Guidelines on the Filing of Standard Contracts for the Outbound Transfer of Personal Information (Second Edition), effective from 22 March 2024; and
- Guidelines on Application of Security Assessment of Cross-border Data Transfers (Second Edition), effective from 22 March 2024.

The Decision has the same legal effect as law, and its purpose is to protect online information security, safeguard the lawful rights and interests of citizens, legal entities or other organizations, and ensure national security and public interests. While the PIS Specification and other Guidelines are only technical guides (covering in detail key issues such as data transfers, sensitive personal information and data subject rights), and thus not legally binding, they have historically been highly persuasive. Although the PIPL takes precedence over the PIS Specification and other Guidelines, the PIS Specification and the Guidelines are still useful for the purposes of supplementing legislation, especially on any part that has not been addressed by the PIPL, CSL or DSL.

In addition to all of the above:

- provisions found in laws such as the Tort Liability Law have generally been used to interpret data protection rights *as a right of reputation or right of privacy*. However, such interpretation is not explicit. The PRC Civil Code, effective on January 1, 2021 further reinforces the statutory right of privacy for individuals and establishes data protection principles; and
- provisions contained in other laws and regulations may also apply depending on the industry or type of information involved (for example, personal information obtained by financial institutions and e-commerce businesses, personal information collected by telecom or Internet service / content providers, healthcare and genetic information, etc.). Applicability of other laws or regulations (including provincial level laws), such as the PRC Criminal Law, PRC E-Commerce Law, PRC Consumer Rights Protection Law and the new local data laws at a provincial level will invariably depend on the factual context of each case and further independent analysis is recommended.

Given the personal information protection framework is still evolving, and further regulations accompanying the new PIPL and DSL are anticipated to be published in the coming months, it is recommended that organizations continue to monitor the developments of the PRC data protection regulatory framework.

Extra-territorial scope

The PIPL has extra–territorial effect, and applies both to:

- data processing activities within the PRC; and
- processing of PRC residents' data outside of PRC where:
  - for the purposes of providing products or services to PRC residents;
  - for analytics or evaluation of behavior of PRC residents; or
  - for any other reasons as required by law or regulations.

The PIPL applies to both the public and private sectors.

DEFINITIONS

Definition of personal data

The PIPL defines personal information as any kind of information relating to an identified or identifiable natural person, either electronically or otherwise recorded, but excluding information that has been anonymized.

Definition of sensitive personal data

The PIPL defines sensitive personal information as information that, once leaked or illegally used, will easily lead to infringement of human dignity or harm to the personal or property safety of a natural person, including (but not limited to):

- biometric data;
- religion;
- specific social status;
- medical health information;
- financial accounts;
- tracking / location information; and
- minors' data.

NATIONAL DATA PROTECTION AUTHORITY

The PIPL has now clarified that the Cyberspace Administration of China (CAC) is primarily responsible for the overall planning and coordination of personal information protection and related supervision. Prior to the PIPL coming into force, various other legislative and administrative authorities have also claimed jurisdiction over data protection matters, and may continue to play some form of role in the context of personal information protection, such as:

- National People's Congress Standing Committee Ministry of Public Security;
- Ministry of Industry and Information Technology State Administration for Market Regulation; and
- Ministry of Science and Technology.

It is also anticipated that the local Public Security Bureau branches and industry regulators will still have a role in both management and enforcement of data protection; and the TC260 technical committee will continue to have delegated responsibility to publish technical standards.

Notwithstanding the CAC's newly-clarified role, sector-specific regulators, such as the People's Bank of China or the China Banking and Insurance Regulatory Commission, may also monitor and enforce data protection issues of regulated institutions within their sector.

REGISTRATION

Generally, there is no legal requirement in the PRC for data users to register with the data protection authority.

That said, there are specific registration requirements imposed on the sharing and transferring of specific categories of data (e.g. human genetic resources), and proposed filling requirements for security impact assessments (see Cross Border Transfers).

DATA PROTECTION OFFICERS

Under the PIPL, organisations which meet certain data processing volume thresholds (as yet unspecified by the CAC) are required to appoint a Data Protection Officer (DPO), and to register the name(s) and contact details of the responsible person with the relevant data protection authority.

For organisations based outside of the PRC, but processing PRC personal information, a specific representative or organisation within the PRC should be appointed, and details reported to the data protection authority.

Details of how and when the DPO or representative (as the case may be) should be registered is awaited.

Whilst the authorities have yet to announce the volume threshold for DPO requirements applicable under the PIPL, the PIS Specification requires an organization to appoint a data protection officer and a data protection department if the organization:

- has more than 200 employees and its main business line involves data processing;
- processes personal information of more than 1,000,000 individuals, or is estimated to process personal information of more than 1,000,000 individuals; or
- processes sensitive personal information of more than 100,000 individuals.

COLLECTION & PROCESSING

Collection

Consent

In general, express, informed consent is required from the data subject before personal information can be collected, used, transferred or otherwise processed. In certain circumstances, such as collecting or processing sensitive personal information, overseas data transfers and direct marketing, separate consent (i.e. explicit consent specific to the processing activity / transfer (rather than just general consent to the privacy notice, expressed through an affirmative action) is required from the data subject. Collection from individuals under 14 years old is prohibited unless explicit consent is obtained from their legal guardians.

In addition, the PIPL requires separate consent to be obtained for:

- processing sensitive personal information;
- overseas transfers;
- public disclosure of personal information;
- to provide data to another data controller for processing; and
- use of image or identification data collected in public through image or identification device for purposes other than maintaining public security.

Whilst there is no clear definition of what "separate consent" constitutes in practice, it appears to suggest that organisations should avoid bundled or forced consent.

The PIPL also introduced limited circumstances (i.e. lawful bases) in which personal information can be processed without consent, including:

- entering into or fulfilling a contract where the data subject is a named party;
- carrying out human resources management under an employment policy legally established or a collective contract legally concluded;
- fulfilling legal obligations (which may be helpful in the context of regulatory investigations);
- protecting the interests of natural person during any public health emergency or otherwise responding to a public health emergency, or in an emergency to protect the safety of natural persons’ health and property;
- carrying out news reporting and public opinion monitoring for public interests;
- the personal information being processed is already made public legally and the processing is within the reasonable scope and in accordance with the requirements of the PIPL; and
- as required by law (e.g. where required to disclose information under another PRC law).

However, in practice, it is unclear how these lawful bases could be relied upon. Consent remains the primary basis for lawful data processing, and it is anticipated this will continue in practice.

Notice

In addition to obtaining consent, a data controller (i.e. the organization who has the authority to determine the purposes, means or method of processing) should provide data subjects with a privacy policy or other form of notice, informing them of the scope and ways in which their personal information is collected, processed and disclosed, including the following information:

- the identity of the data controller, including its registered name, registered address, principal office, a telephone number and / or an e-mail address;
- a list of personal information collected for each business purpose. Where sensitive personal information is involved, relevant consent shall be explicitly marked or highlighted;
- the location of storage, retention period, means of use / processing and scope of the personal information collected; the purposes sought by the data controller, i.e. what the data controller uses the data for (for instance, supplying goods and services, creating a user account, processing payments, managing subscriptions to the newsletters, etc.). These should be as comprehensive as possible, as additional purposes will require new consent;

- circumstances under which the data controller will transfer, share, assign personal information to third party processors (including intra-group entities) or publicly disclose personal information, the types of personal information involved in these circumstances, the types of third party data recipients, and the respective security and legal responsibilities of the entities;
- circumstances under which the data controller will transfer, share or assign personal information to third party controllers, the names and contact information of third party controllers, purpose and means of processing and personal information categories;
- circumstances under which the personal information will be transferred, accessed or stored outside of the PRC, the names and contact information of overseas recipients, purpose and means of processing, personal information categories and the means and procedures for individuals to exercise their data subject rights against the overseas recipients;
- the rights of data subjects and mechanisms for them to exercise such rights, e.g. methods to access, rectify or delete their personal information, to de-register their accounts, withdraw their consent, obtain copies of their personal information and restrict automated decision by the data system etc.;
- potential risks for providing personal information, as well as possible consequences for not providing the data; data security capabilities of, and data security protection measures to be adopted by, the data controller and, when necessary, the compliance certificates related to data security and personal information protection; and
- channels and procedures for making inquiries and lodging complaints by data subjects, as well as external dispute settlement body and contact information.

The information in the privacy policy must be true, accurate and complete. The contents of the privacy policy must be clear and easy to understand, and ambiguous language should be avoided. The privacy policy should be made available to the data subject when collecting consent, and published publicly and easily accessible, for example, through a link placed prominently on a webpage or an installation page of a mobile application. When changes occur to the information provided in the privacy policy, the data subjects should be notified of such changes and (depending on the extent of changes made) further consent may need to be obtained.

Processing

Collection and processing of personal information must be directly related to the purpose of processing specified in the privacy notice.

Excessive data collection must be avoided. Interestingly the provisions of the PIPL around data minimization appear to be targeted at apps and big data analytics. On March 1, 2022, the Administrative Provisions on Recommendation Algorithms in Internet-based Information Services came into effect, which require recommendation algorithm-based service providers to establish management systems and technical measures for data security and personal information protection.

Additional restrictions are placed on use of biometric data collected in public places.

There are prohibitions on illegal collection, use, processing, sale, disclosure and transfer of personal information.

Impact assessment and record-keeping

The PIPL requires data controllers to undertake personal information impact assessments (PIIA) and to retain the results and processing records (for three years) in the following circumstances:

- processing of sensitive personal information;
- using personal information to conduct automated decision-making;
- appointing a data processor;
- providing personal information to any third party (likely to include sharing with group companies);
- public disclosure of personal information;
- overseas transfer of personal information; and
- any other processing activities that may have "significant impact to an individual".

A PIIA should include an assessment on:

- whether the purpose of use and means of processing is legitimate, proper and necessary;
- impacts and risks to individual's interests; and
- applicability of protection measures and risk appetite.

The "Guidance for Personal Information Security Impact Assessment" (PIIA Guidelines) (published by the National Standardization Technical Committee for Information Security) came into force on June 1, 2021.

TRANSFER

If a data controller wishes to share, disclose or otherwise transfer an individual's personal information to a third party (including group companies), the data controller must:

- if the third party is a separate data controller, inform the data subject of the purposes of the sharing, disclosure or transfer of the personal information the types of data shared, the name and contact information of the recipient, and obtain prior separate consent from the data subject;
- perform a personal information impact assessment (PIIA), and take effective measures to protect the data subjects according to the assessment results (e.g. putting in place a data transfer agreement or similar contractual protections) (see Collection & Processing);
- record accurately and keep the information in relation to the sharing, disclosure or transfer of the personal information, including the date, scale, purpose and basic information of the data recipient of the sharing or assigning;
- ensure personal information is only transferred where required for processing purposes; not share or transfer any personal biometric information or other types of particularly sensitive personal information where prohibited under relevant laws or regulations; and
- ensure contractual measures are entered into to require the data processor to comply or assist the data controller in complying with obligations under data protection laws.

Cross-border transfers

Most personal information can be transferred or accessed outside of the PRC providing the following compliance steps are taken:

- the data controller has completed one of the following mechanisms to legitimize overseas data transfer, unless the transfer is exempted from such requirement — for details please see below:
    - the organisation has passed a CAC security assessment;
    - the organisation has obtained certification from a CAC-accredited agency;
    - the organisation has put in place CAC standard contractual clauses (SCCs) with the data recipient and filed the signed SCCs with the local CAC together with a cross-border transfer specific PIIA report; or
    - for compliance with laws and regulations or other requirements imposed by the CAC;
- the data controller has adopted necessary measures to ensure the data recipient's data processing activities comply with standards comparable to those set out in the PIPL. In practice this means initial due diligence, sufficient contractual protections and ongoing monitoring etc.;
- notice and separate, explicit consent has been given / obtained (see above) from the data subject (see Collection & Processing); and
- a PIIA has been conducted (see Collection & Processing).

1. Exempted Transfers

According to the Regulations on Facilitating and Regulating the Cross–border Data Transfers, the following cross-border data transfers are exempted from having to follow any one of the legitimising mechanisms above ("Exempted Transfers”):

- Collection outside of PRC the personal information being transferred outside of PRC was originally collected and generated outside of PRC and thereafter imported back into PRC, and the processing of such personal information within PRC does not involve any personal information or important data that is collected from or generated in PRC;
- Cross-border HR management: the transfer is necessary for implementing cross-border human resource management in accordance with legally formulated employment policies and procedures or legally executed collective contracts;

- Cross-border contract: the transfer is necessary for concluding or performing a contract between the data subject and the data controller (e.g. those contracts that relate to cross-border shipping, logistics, remittance, payments, bank account opening, flight and hotel booking, visa applications, examination services etc.); or
- Emergency situation: the transfer is necessary for protecting the life, health or property security of any natural person under emergency circumstances.

Exempted Transfers 2 (cross-border HR management) and 3 (cross-border contracts) above rely on a “necessity” test. This means the organisation must prove that the cross-border data transfer is necessary in order for the exemption to apply. However, it remains unclear as to what would constitute a necessary basis for the cross-border transfer of personal information.

After carving out all the Exempted Transfers, the data controller shall determine the applicable mechanisms to legitimise the rest overseas data transfers as follows:

2. CAC security assessment

According to the Regulations on Facilitating and Regulating the Cross–border Data Transfers, a CAC security assessment is required for data controllers who meet any of the following thresholds:

- an organisation intends to transfer any "important data" overseas;
- a CIIO intends to transfer any personal information overseas;
- a data controller intends to transfer non-sensitive personal information of more than 1,000,000 individuals overseas since 1 January of the year when the calculation is conducted; or
- a data controller intends to transfer sensitive personal information of more than 10,000 individuals overseas since 1 January of the year when the calculation is conducted.

The CAC security assessment involves the organisation completing a self–assessment of its cross-border data transfers, which must then be submitted for approval by both the local and national CAC. It primarily assesses the impact of overseas transfers on national security, public interest, and the legitimate rights and interests of individuals or organisations. If the CAC security assessment is passed, the organisation will be granted with a written approval. Such approval will be valid for 3 years and could be extended for another 3 years upon approval by both the local and national CAC, provided the organisation has made no change to its previously approved cross–border transfers.

For organisations that must follow the CAC security assessment route, a copy of the data must in practice be stored locally in the PRC.

3. China SCCs

According to the Regulations on Facilitating and Regulating the Cross–border Data Transfers, a China SCCs filing with the CAC is required for data controllers who meet any of the following thresholds:

- a data controller intends to transfer non-sensitive personal information of between 100,000 and 1,000,000 individuals overseas since 1 January of the year when the calculation is conducted; or
- a data controller intends to transfer sensitive personal information of fewer than 10,000 individuals overseas since 1 January of the year when the calculation is conducted.

For PRC data controllers that must follow the China SCCs filing route, they must put in place the China SCCs with the overseas data recipient, and then within 10 working days after the effectiveness of the China SCCs file a copy of the signed SCCs together with the corresponding PIIA with the local CAC.

The Measures for the Standard Contract for the Outbound Transfer of Personal Information and the Guidelines on the Filing of Standard Contracts for the Outbound Transfer of Personal Information (Second Edition) provide clarification on how the SCCs may be implemented by organisations as one of the mechanisms for overseas data transfer under the PIPL, how to prepare the corresponding PIIA by using the standard template formulated by the CAC and the procedures for filing the signed SCCs and the PIIA report.

4. CAC certification

The CAC certification route applies to organisations who trigger the same thresholds as the China SCCs. However, there remains uncertainty around its applicability. According to the Practicing Guidelines for Network Security Standards — Technical Specification for Certification of Personal Information Cross–border Processing Activities (V2.0), it will once implemented set up a framework of certification of overseas data transfer, including the principles, data protection obligations of data controllers and the overseas recipient, ensuring data subject rights, etc. Details to implement the certification remain unclear.

Organisations within regulated industry sectors may have to follow other compliance steps prescribed by their industry regulator to transfer or remote access their personal information outside of the PRC.

However, certain personal information (and non–personal information) must still remain in (and cannot be accessed outside of) the PRC. This includes (this is not an exhaustive list):

- certain data under industry–specific regulations (such as in the financial services sector and genetic health data); and
- certain restricted data categories (such as "state secrets", some "important data", geolocation and online mapping data etc.).

The Draft Network Data Security Management Regulation also proposes introducing annual data overseas transfer security report to the CAC as well as other record keeping requirements.

Finally, according to the PIPL:

- a new publicly–available entity list may be published, listings foreign organisations to whom local PRC organisations may not transfer personal information, where such transfer may harm national security or public interest; data controllers must not provide personal information stored within the PRC to overseas legal or enforcement authorities unless approval is obtained from a designated Chinese authority. It remains unclear whether this extends to, say, requests from overseas industry regulators; and
- the PIPL clarifies that Chinese authorities may provide personal information stored within the PRC to overseas legal or enforcement authorities upon request, if and to the extent that there are international treaties or regulations in place to maintain fairness and for mutual benefit.

5. Transfer of personal information within the Greater Bay Area

Given the close integration of cities within the Guangdong–Hong Kong–Macao Greater Bay Area (GBA), and that data flows between Hong Kong and other cities within the GBA are becoming increasingly frequent, the CAC and the Innovation, Technology and Industry Bureau of the Government of the Hong Kong Special Administrative Region (ITIB) and Office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD) together formulated the Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong– Hong Kong–Macao Greater Bay Area (Mainland, Hong Kong) (GBA SCCs).

In addition to complying with other general data protection requirements (e.g. notice, consent and impact assessment, etc.) if the data controller and the data recipient are registered in Guangzhou, Shenzhen, Zhuhai, Foshan, Huizhou, Dongguan, Zhongshan, Jiangmen, Zhaoqing or Hong Kong SAR, they may consider signing the GBA SCCs to legitimize the transfer and file the signed GBA SCCs with the Guangdong CAC and PCPD.

SECURITY

According to the CSL, DSL and PIPL, organizations must keep personal information confidential and establish a data security management system. This includes taking appropriate technical and organizational measures against unauthorized or unlawful processing and against accidental loss, destruction of, or damage to, personal information. The measures taken must ensure a level of security appropriate to the harm that may result from such unauthorized or unlawful processing, accidental loss, destruction or damage, and appropriate to the nature of the data. Security measures must be deployed, as prescribed by the CSL and DSL and their underlying measures, guidelines and technical standards (including the TC260 guidelines). The PIPL includes a

specific obligation on data controllers to adopt corresponding encryption or deidentification technologies, and to adopt access controls and training.

Systems should also be established to handle complaints or reports about personal information security, publish the means for individuals to make such complaints or reports, and promptly handle any such complaints or reports received. Organizations must conduct mandatory data / cyber security training.

Additional security safeguards must be applied to processing of sensitive personal information and organizations deemed CIIOs (see above).

The CSL implemented a multi-level protection scheme for cybersecurity protection of information systems by network operators. Information systems are classified into 5 tiers and the security standard goes higher from tier 1 to tier 5. Organizations should conduct a self-evaluation and determine the tier(s) to which its information systems belong, based on relevant laws, regulations and guidelines. Filing to the Public Security Bureau is required and, in certain circumstances, assessment by accredited third party may also be required, depending on the determined tier level of a respective information system. Further national standards and guidelines have been published to provide further details and requirements on the process and technical aspect of the tiered system.

The DSL proposes introducing a similar tiered-security scheme for classification of data in due course (details have not yet been published).

Industrial regulators in each sector are working on issuing the data classification scheme in the relevant sectors. In particular, the Ministry of Industry and Information Technology recently issued the Measures for Data Security Management in the Industrial and Information Technology Sector (for Trial Implementation) (MIIT Measures) which came into force on January 1, 2023. The MIIT Measures provide standards for data classification and grading scheme in the industrial and information technology sector and classify data into three grades: general data, important data, and core data. Additionally, the Draft National Standard of Information Security Technology — Requirements for Classification and Grading of Network Data provides the principles and methods for data classification and grading.

If a data controller appoints a data processor to process personal information on its behalf, the data controller should ensure sufficient measures are adopted by the data processor to protect the personal information: for example, to conduct due diligence and regular audits on data processor to ensure the data processor adopts sufficient and adequate security measures; and put in place an appropriate data processing agreement with the data processor.

BREACH NOTIFICATION

Breach notification requirements are contained in the CSL, DSL and PIPL, and should be read together. "Network security incidents" that are notifiable are defined by reference to seven categories of different incident types, in particular:

1. Malicious program incidents;
2. Network attack incidents;
3. Data security incidents;
4. Information content security incidents;
5. Equipment and facility failure incidents;
6. Operational violation incidents;
7. Security risk incidents;
8. Abnormal behavior incidents;
9. Force majeure incidents; and
10. Other cyber incidents.

Guidelines set out other factors that should be considered whether a network security incident is potentially reportable. The China National Internet Emergency Center may be contacted in case of doubt as to whether an incident is potentially reportable.

An incident must be immediately notified: (i) internally, to the DPO; and (ii) externally, to the regulator (the PIPL refers to the CAC establishing (local) "personal information protection departments" (PIPD) for such purposes, but this is yet to be confirmed), and should include:

- affected data categories;
- reasons for the incident, and potential consequences;
- remedial measures, and mechanisms required by data controller to minimize impact; and
- contact information for data controller.

If the data controller can effectively avoid the disclosure, loss or tampering of data, the PIPL suggests that there is no need to notify data subjects. Otherwise (and as per the CSL and DSL) data subjects must be notified immediately if the actual or suspected network security incident may result in harm to the rights and interest of the affected data subjects. Further, if the PIPD believes it may cause impact to individuals, they may request that the data controller notifies individuals. Similar information must be given to the data subjects alongside advice on how to protect against risks arising from the incident.

Further changes are also expected in this regard. Notably, the Draft Network Data Security Management Regulation (intended to supplement the PIPL) clarifies that incidents involving any of the following must be notified to the CAC and other relevant regulators within eight hours of the data incident:

- personal information of more than 100,000 individuals; or
- any important data.

A second report to the CAC is then required within five working days of the incident being resolved.

In any case, immediate remedial action must be taken in the event of any suspected or actual data disclosure, loss or tampering.

Organizations should also adopt proactive measures to minimize the risk of personal information breaches or security incidents, including but not limited to, implementing and testing a data incident contingency plan and organizing training.

We understand the regulators are working on a project to publish further guidelines as to how network security incidents should be managed. On 8 December 2023, the CAC released the Draft Administrative Measures on Cybersecurity Incident Reporting to solicit public opinions. This draft proposes new mechanisms to classify cybersecurity incidents and new reporting obligations.

ENFORCEMENT

Possible enforcement of, and sanctions for, a data protection breach in the PRC will depend on the specific data protection laws and regulations breached. Sanctions in relation to data protection breaches are scattered across various different laws and regulations, and the measures described below may not be comprehensive in all situations, as additional laws or regulations may be applicable depending on the industry or type of information at hand.

Taking the PIPL by way of example, it provides a range of sanctions, including (*inter alia*):

- enforcement notices and warnings;
- administrative fines of up to (for the most serious offences) 5% of the previous year's annual revenue (unclear if local or
- global revenue) or up to RMB million, and confiscation of unlawful income. Note the PIPL imposes much higher fines than
- under other existing data privacy regulations);
- cessation of processing;
- suspension of apps and / or services;
- suspension of business;
- suspension of management / officials role;
- criminal sanctions (for certain offences, and under relevant criminal laws);
- civil claims; and
- social credit score or equivalent business credit files may be affected.

While the PIPL has now introduced higher fines, we anticipate that in practice the operational and contractual risks faced by organisations not complying with the PRC's data privacy framework — alongside increasing reputational risks — remain very significant and should be managed very carefully.

ELECTRONIC MARKETING

Direct marketing by electronic means is only possible if the targeted consumers have explicitly consented to receiving such messages either at the time their electronic address / mobile phone number was collected or at a later time.

Specific information must be stated in each electronic message: for example, the identity of the entity sending the message, and a mark identifying "*Guang gao*" (which means advertisement in Chinese) or "AD" on a direct marketing message.

There are also specific rules applicable to direct marketing by text messages (SMS), and certain specific prescribed information must be provided to data subjects at the time their mobile phone number was collected or prior to sending direct marketing text messages.

ONLINE PRIVACY

The general compliance obligations applicable to processing of personal information under the PIPL apply to the online (and offline) environments. In addition, the PIPL imposes additional compliance obligations on organisations that fall into one of the following categories:

- "important internet platform providers";
- data controllers processing data of a "large volume of users"; or
- "complex businesses".

It is still unclear which organisations would fall within these categories, but these organisations must comply with additional measures when processing personal information, namely:

a. set up personal information protection compliance mechanisms;
b. set up external independent data protection organisations to supervise data protection mechanisms;
c. establish platform regulations;
d. establish and publish processing obligations and processing rules that regulate products and service providers in an open and fair manner;
e. stop the provision of products or service providers if they violate the law or regulations as regards processing of personal information; and
f. publish from time to time social responsibility reports as regards processing of personal information.

In terms of automated–decision making and profiling:

- analytics or evaluation based on computer programme around behavior, interests, hobbies, credit information, health or decision making activities, must be transparent, open and fair, and should not apply any differential treatment between individuals; and
- any push information or business marketing should not be directed to an individual's character and should provide individuals with a convenient way to opt out.

As well as the PIPL, the CSL, Consumer Protection Law and E–Commerce Law offer protection to consumer / user personal information. As well as personal information protection, under these rules data controllers should strengthen management of information provided by users, prohibit the transmission of unlawful information and take necessary measures to remove any infringing content, then report to supervisory authorities. Sufficient notice and adequate consent should be obtained from data subjects prior to the collection and use of personal information. Further obligations are imposed on mobile apps providers including but not limited to conducting real–name identification, undertaking information content review.

In recent years, the regulators have also issued a range of guidelines targeting mobile app providers. These guidelines introduce specific data protection and privacy obligations aiming to regulate the data collection practices and processing activities of mobile app providers. There has also been a crackdown against (suspected) non–compliant mobile apps. Organisations are advised to review their app compliance as a matter of priority.

Data subject rights (under the PIPL and other laws within the personal information framework), include rights to access and obtain information about their data held and processed, to correct their data, to request deletion of data in the event of a data breach, to object to automated decision–making and to de–register their account etc. Most importantly is the right to withdraw consent to personal information processing.

There are currently no specific requirements regarding cookies within existing laws or regulations in the PRC. However, the use of cookies and / or similar tracking technologies, to the extent they constitute processing of personal information, should be notified to data subjects as part of a privacy policy and adequate consent should be obtained from data subjects for such use.

KEY CONTACTS

Carolyn Bigg
Partner, Global Co-Chair of Data Protection, Privacy and Security Group
T +852 2103 0576
carolyn.bigg@dlapiper.com

Venus Cheung
Registered Foreign Lawyer
T +852 2103 0572
venus.cheung@dlapiper.com

Amanda Ge
Of Counsel
DLA Piper
T +86 185 1511 8230
amanda.ge@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

COLOMBIA

Last modified 28 January 2024

LAW

Colombia recognizes two fundamental personal data rights under Articles 15 and 20 of its Constitution: (1) the right to privacy and (2) the right to data rectification. Personal data processing is further regulated by two statutory laws and several decrees that set out data protection obligations.

Statutory Law 1266 of 2008 (Law 1266) regulates the processing of financial data, credit records and commercial information collected in Colombia or abroad. Law 1266 defines general terms on habeas data and establishes basic data processing principles, data subject rights, data controller obligations and specific rules for financial data.

Law 1266 defines the terms Data Subject, Data Source, User of Data and Data Operator, as follows:

- ‘Data Subject’ means the owner of the information;
- ‘Data Source’ means a person or entity who receives or collects the information in the context of a commercial relationship with the Data Subject and shares this information with the Data Operator;
- ‘User of Data’ means a person or entity who accesses databases and uses the information gathered by the Data Operator;
- ‘Data Operator’ means a person who manages a database with information provided by the Data Sources and shares it with Users of Data, under the rules provided by Law 1266. The most common example of a Data Operators is a Credit Bureau.

Law 1266 provides the applicable rules and conditions for Data Sources to share information with Data Operators and for such Data Operator to manage and share the information with Users of Data. Notwithstanding this, the Law privileges processing for purposes of managing financial, credit, commercial and services information, considering that this benefits the financial and credit activity as a public interest activity.

Law 1266 was amended by Law 2157 of 2021. The main modifications introduced by Law 2157 are the following:

- Data whose content refers to the time of default of an individual or a company, or data that refers to a lack of compliance with monetary obligations, shall be erased immediately or as promptly as possible. This erasure requirement applies mainly to small companies, small farmers, armed conflict victims, young people, women from rural areas, and other debtors who are in special situations, with the specificities foreseen in the Law.
- The obligation to update credit scores was created, provided that any negative data is erased.
- The Law established that the frequent consultation of a person’s credit history should not be a factor for lowering their credit rating.
- Claims and requests concerning the processing of financial data must be resolved within fifteen (15) working days from the date of receipt of the communication. If a prompt resolution is not given within this timeframe, the request is presumed accepted for all legal purposes.
- Financial data, credit records, and commercial information may not be used in making employment decisions.

- The Law introduced the principle of accountability for the processing of financial information. This update implies the Data Source and the Data Operator should adopt internal policies to guarantee the safety and confidentiality of the information.

Furthermore, Statutory Law 1581 of 2012 (Law 1581) regulates all personal data processing, as well as databases. Law 1581 defines special categories of personal data, including sensitive data and data collected from minors. Under the law a ‘Data Controller’ is a legal or natural person responsible for data treatment, or processing, and a ‘Data Processor’ is a legal or natural person in charge of personal data processing. The Data Controller creates databases on its own or in association with others, while the Data Processor processes personal data on behalf of the Data Controller. Nevertheless, an entity may be regarded as both Controller and Processor of personal data.

The law further regulates the obtention of authorization to treat personal data and the procedures for data processing. Moreover, the law creates the National Register of Data Bases (NRDB).

Law 1581 is applicable to all data collection and processing in Colombia, except data regulated under Law 1266 and certain other types of data or regulated industries. The law is further applicable in any case where a data processor or controller is required to apply Colombian law under international treaties.

Law 1581 does not regulate:

- Databases regulated under Law 1266;
- Personal or domestic databases;
- Databases aimed to protect and guarantee national security, prevent money laundering and terrorism financing;
- Intelligence and counter-intelligence agency databases;
- Databases with journalistic information and editorial content; and
- Databases regulated under Law 79 of 1993 (on population census).

Law 1581 further requires Data Controllers and Data Processors to guarantee that personal data: is maintained pursuant to strict security measures and confidentiality standards, will not be modified or disclosed without the data subject’s consent, and will only be used for purposes identified in a privacy policy or notice.

Decree 1377 of 2013 (Decree 1377), is a piece of secondary regulation related to Law 1581 which outlines requirements for personal and domestic databases regarding authorization of personal data usage and recollection, limitations to data processing, cross-border transfer of data bases and privacy warnings, among others. This Decree also requires controllers and processors to adopt a privacy policy and privacy notice.

Decree 886 of 2014 (Decree 886) and Decree 090 of 2018 (Decree 090) issued by the Ministry of Commerce, Industry and Tourism, regulate the National Register of Data Bases and sets deadlines for registration of existing data bases in Colombia.

Lastly, Title V of the Sole Circular issued by the Superintendence of Industry and Commerce provides additional guidelines regarding the following matters: (i) the processing of financial data, credit records and commercial information; (ii) the National Register of Data Bases and (iii) International Data Transfers.

DEFINITIONS

The Colombian data protection regime distinguishes between personal data and a sub-category of sensitive personal data, depending on the information and the harmful effects caused by its unlawful use. Law 1266 and Law 1581 contain particular rules related to sensitive personal data.

Definition of personal data

Under Law 1266, personal data is defined as any information related to or that may be associated with one or several determined or determinable natural or legal persons. Personal data may also be regarded as public, private or semi-private data. Public data is available to the public based on a legal or constitutional mandate. Private or semi-private data is data that does not have a public purpose, is intimate in nature and the disclosure of which concerns only the data subject.

Under Law 1581, personal data is defined as any information related to, or that may be related to, one or several determined or determinable individuals, meaning natural persons only.

Definition of sensitive personal data

Under Law 1266, sensitive personal data is defined as data that due to its sensitivity is only relevant to its owner.

Under Law 1581, sensitive personal data is any data that affects its owner’s intimacy or whose improper use might cause discrimination. Data that reveals any of the below information is considered sensitive data and its processing is prohibited by law:

- Ethnic or racial origin
- Political orientation
- Religious or philosophic convictions
- Membership in labor unions, human right groups or social organizations
- Membership in any group that promotes any political interest or that promotes the rights of opposition parties
- Information regarding health and sexual life, and
- Biometrics

Sensitive personal data shall only be processed:

- With the Data Subject's special and specific consent
- If necessary to preserve the data subject’s life, or a vital interest and the Data Subject is physically or legally unable to provide consent
- If used for a legitimate activity and with all necessary security measures, by an NGO, an association or any kind of nonprofit entity, in which case, the entity will need the Data Subject's consent to provide the sensitve personal data to third parties
- If such data is related to or fundamental to exercising a right in the context of a trial or any judicial procedure, or
- If such data has a historic, statistical or scientific purpose, in which case the Data Subject's identity may not be disclosed

NATIONAL DATA PROTECTION AUTHORITY

According to Law 1266, there are two different authorities on data protection and data privacy matters. The first of them, which acts as a general authority, is the Superintendent of Industry and Commerce (SIC). The second authority is the Superintendence of Finance (SOF), which acts as a supervisor of financial institutions, credit bureaus and other entities that manage financial data or credit records and verifies the enforcement of Law 1266.

Nevertheless, under Law 1581, the SIC is the highest authority regarding personal data protection and data privacy. It is empowered to investigate and impose penalties on companies for the inappropriate collection, storage, usage, transfer and elimination of personal data.

REGISTRATION

Law 1581 created the National Register of Data Bases (NRDB). Databases that store personal data and whose automated or manual processing is carried out by a natural or legal person, whether public or private in nature, in the Colombian territory or abroad, shall be registered in the NRDB. Database registration is also required if Colombian law applies to the data controller or data processor under an International Law or Treaty. Registration is mandatory for data controllers that are either of the following:

- Companies or nonprofit entities that have total assets valued above 100,000 Tax Value Units (TVU), meaning COP 3.800.400.000 million (USD 950.100)[1]
- Legal persons of public nature

Decree 866 states that each data controller shall register each one of its databases, independently and must distinguish between manual and automatized databases. In addition, in order to register each database, the data controller or data processor shall provide the following information:

- Identification information of the data controller, such as: business name, tax identification number, location and contact information
- Identification details of the data processor, such as: business name, tax identification number, location and contact information
- Contact channels to grant data subjects rights
- Name and purpose of the database
- Form of processing (manual / automatized)
- Security standards
- Privacy policy

All data bases were required to register by January 31, 2019. Any new data base(s) shall be registered within the 2 months following its creation.

Any substantial change to any of the abovementioned items, shall be updated in the National Registry of Data Bases. For this purpose, substantial changes are considered as any changes that are made in regards to the purposes of the databases, the data processors, the channels to process any claim or request from the data subject, the class or type of personal data, the security measures implemented, the data privacy policy and/or the international transfer or transmission of personal data.

Such updates shall be made:

i. Within the 10 first days of the month in which the substantial change was made,

and

ii. Yearly (between January 2 and March 31 of each year).

Moreover, through the National Register of Data Bases, data controllers shall inform of the following:

i. Any claim submitted by a data subject to the data controller and/or data processor, within each semester of the year. This information shall be registered within the first 15 business days of February and August of each year with the information of the previous semester.
ii. Any breaches of registered data bases. Such report shall be submitted within the 15 business days following the day on which the data controller had knowledge of the data breach.

Footnote 1: Based on the Tax Value Unit for 2022 (COP $38.004 (approximately USD 9.5)). The Tax Value Unit is updated yearly by the Colombian tax authority.

DATA PROTECTION OFFICERS

There is no requirement to appoint a formal data protection officer in Colombia. However, companies are required to appoint either a specific person, or a designated group within the company to be in charge of personal data matters, specifically the handeling of Data Subject rights and privacy request .

COLLECTION & PROCESSING

The processing of financial data, credit records and commercial information, collected in Colombia or abroad, does not require authorization from the Data Subject. However, this information may only be disclosed to:

- The Data Subject or authorized third parties, pursuant to the procedure established by law
- The Users of the Data
- Any judicial or jurisdictional authority upon request
- Any control or administrative authority, when an investigation is ongoing

- Data processors, with the Data Subject’s authorization, or when no authorization is needed , and the database aims for the same objective or involves an activity that may cover the purpose of the disclosing data processor

On the contrary, Law 1581, requires the authorization of the Data Subject for the data controller to process private and semi-private personal data. For the authorization to be valid it must be obtained prior to the data processing and must be "informed", meaning that the data subject must have been made aware of the exact purposes for which the data is being processed. Decree 1377 requires the following:

- Personal data shall only be collected and processed in accordance with the purposes authorized by the Data Subject.
- Such authorization may be obtained by any means, provided that it allows subsequent consultation.

Authorization is not required when:

- A public or administrative entity demands the information through a judicial order or exercising its legal duties.
- It is public data.
- A medical or sanitary urgency requires the processing of personal data.
- The data processing is authorized by law for historical, statistical or scientific purposes.
- The data is related to people’s birth certificates.

Regarding sensitive personal data, Section 6 of Decree 1377 states that the data controller shall do the following:

- Expressly inform the Data Subject that he or she is not compelled to provide sensitive personal data
- Expressly identify what data to be collected and processed is sensitive and
- Obtain the Data Subject's express consent prior to the processing of their sensitive personal data

In any case, silence is not considered a reasonable means of obtaining authorization for personal data or sensitive personal data processing.

Furthermore, when collecting personal data of children, both the data controller and the data processor shall ensure that personal data processed serves and respects the children’s superior interests and guarantees their fundamental rights. For these purposes, the child's legal representative (parent or guardian) must authorize the processing of their child’s personal data.

Privacy policy and privacy notice

Decree 1377 establishes the obligation for data controllers to develop a privacy policy that governs personal data processing and ensures regulatory compliance. For this reason, privacy policies are mandatory for all data controllers and shall be clearly written; Spanish is recommended. Finally, according to the Decree 1377, the minimum requirements for the privacy policy are:

- Name, address, email and phone number of the data controller
- Processes and handling of data and the purpose of such processing
- Rights of the Data Subject
- Individual or department within the data controller that is responsible for the attention to requests, consultations and claims to update, rectify or suppress data and to revoke authorization
- Procedure to exercise the abovementioned rights, and
- Date of creation and effective date

The privacy notice is a verbal or written communication by the data controller, addressed to the data subject, for processing her /his personal data. In this communication, the data subject is informed about the privacy policies of the data controller, the manner to access them and the purposes of the treatment.

TRANSFER

Per Law 1581, the transfer of personal data occurs when the data controller or the data processor located in Colombia sends the personal data to a recipient, in Colombia or abroad, who is responsible for the personal data, *ie*, a data controller.

Cross-border data transfers are prohibited unless the country where the data will be transferred to provides at least equivalent data privacy and protection standards and adequate safeguards to those provided by Colombian law. In this regard, adequate levels of data protection will be determined in accordance with the standards set by the SIC.

This restriction does not apply in the following cases:

- If the Data Subject expressly consented to the cross-border transfer of data
- Exchange of medical data
- Bank or stock transfers
- Transfers agreed to under international treaties to which the Colombia is a party
- Transfers necessary for the performance of a contract between the Data Subject and the controller, or for the implementation of pre-contractual measures, provided the data owner consented, and
- Transfers legally required in order to safeguard the public interest

Therefore, the data controller requires the authorization of the Data Subject for transferring the personal data abroad, unless such transfer is to one of the following countries which, according to the SIC, meet the standard of data protection and security levels.

Authorized countries for international transfer of personal data

- Albania
- Argentina
- Austria
- Belgium
- Bulgaria
- Canada
- Costa Rica
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungry
- Iceland
- Ireland
- Italy
- Japan
- Latvia
- Lithuania
- Luxembourg
- Malta
- Mexico
- Netherlands
- New Zealand
- Norway
- Perú
- Poland
- Portugal
- Republic of Korea

- Romania
- Serbia
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- United States
- United Kingdom
- Uruguay

The SIC also considers that personal data can be transferred to any country regarding which the European Commission considers to meets its standard for levels of protection.

Transfer of personal data

The transfer of personal data takes place when the data controller provides personal data to a data processor, in Colombia or abroad, in order to allow the data processor to process the personal data on behalf of the data controller. The data subject’s consent is required for the transfer of data, unless an adequate data transfer agreement between the data processor and the data controller is in place.

In this regard, Decree 1377 requires that the aforementioned agreement include the following clauses:

1. The extent and limitations of the data treatment
2. The activities that the data processor will perform on behalf of the data controller, and
3. The obligations the data processor has to data subjects and the data controller

The data processor has three additional obligations when processing personal data:

- Process data according to the legal principles established in Colombian law
- Guarantee the safety and security of the databases
- Maintain strict confidentiality of the personal data

A data controller transferring data to a data processor must identify the data processor in the National Database Register for each database transferred. Finally, the data processor must process the personal data in accordance with the data controller’s privacy policy and the authorization given by the data subject.

SECURITY

Data controllers have the legal duty of guaranteeing that the information under their control is kept under strict security measures. For this reason, data controllers shall ensure that such information will not be manipulated or modified without the Data Subject's consent . For this purpose, the data controller shall develop an information security policy that prevents the unauthorized access, the damage or loss of information, including personal data.

BREACH NOTIFICATION

In accordance with Chapter 2, Title V of the Sole Circular issued by the SIC, a data breach refers to the violation of security codes or to the loss and unauthorized access of data subjects’ information held in a database managed by data controllers or data processors.

Under section 17. and section 18. of Law 1581, both the data controller and the data processor have a duty to notify the authority (SIC) in case of a breach of security, security risk, or a risk for data administration. Such notification shall be made no later than fifteen (15) business days from the date on which the data breach was detected.

Lastly, the Colombian data protection regime does not provide a threshold for data breach notifications. Hence, if there is a violation to the security codes or a risk in the management of data subjects’ information, data controllers and data processors must notify the breach.

ENFORCEMENT

Since privacy and proper maintenance of personal data are fundamental constitutional rights in Colombia, every citizen is entitled to pursue protection before any Colombian judge, via constitutional action. Any judge may order a private or public entity to modify, rectify, secure or delete personal data if it is kept under conditions that violate constitutional rights. Constitutional actions can take up to ten days to be resolved and an order issued and failure to comply may result in imprisonment of the legal representative of the violating entity.

The Criminal Code of Colombia sets out in section 269F that anyone who, without authorization, seeking personal or third party gain, obtains, compiles, subtracts, offers, sells, interchanges, sends, purchases, intercepts, divulges, modifies or employs personal codes or data contained in databases or similar platforms, will be punishable by 48 to 96 months of prison, and a fine of approximately USD 26,700 to USD 267,000.

Finally, since SIC is an administrative and jurisdictional authority, it is allowed to investigate (as mentioned above), request information, initiate actions against private entities, and impose fines up to approximately USD 534,000, and order or obtain temporary or permanent foreclosure of the company, entity or business.

ELECTRONIC MARKETING

Law 527 of 1999 (Law 527) regulates e-commerce and electronic marketing, but there is no specific regulation regarding data privacy on electronic marketing. In any case, the Data Subject's consent is required for marketing, whether electronic or not and the processing of any personal data for this purpose shall be in accordance with Law 1581.

ONLINE PRIVACY

There is no specific regulation regarding online processing of personal data. Thus, online privacy and data processing is governed by Law 1581.

Personal data must not be available online unless there are adequate security measures to ensure that access by any unauthorized user is restricted.

Collection and use of data collected through cookies or similar online tracking tools is prohibited unless the Data Subject has provided consent. Such consent may be obtained by a pop-up informing the user about the company's privacy policy and ways for the Data Subject's to review, manage or disable cookies.

KEY CONTACTS

Maria Claudia Martinez Beltrán
Partner
DLA Piper Martinez Beltrán
T +57 3174720
mcmartinez@dlapipermb.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

COSTA RICA

Last modified 28 January 2024

LAW

Data privacy regulation in Costa Rica is contained in two laws, the "Laws": Law No. 7975, the Undisclosed Information Law, which makes it a crime to disclose confidential and/or personal information without authorization; and Law No. 8968, Protection in the Handling of the Personal Data of Individuals together with its by-laws, which were enacted to regulate the activities of companies that administer databases containing personal information. Therefore, the scope of the second law is limited.

The Costa Rican Congress is currently discussing a bill, which would fully amend the Laws currently in effect. Such bill was presented to local Congress in January 2021 and is still under discussion.

The proposed bill aims to update the Laws and align its provisions to the principles contained in the EU General Data Protection Regulation (GDPR). It is still unclear when and if the proposed bill will be enacted.

DEFINITIONS

Definition of personal data

Personal information contained in public or private registries (eg, medical records) that identifies or could be used to identify a natural person. Personal information can only be disclosed to persons or entities with a need to know such information.

Definition of sensitive personal data

Personal information related to the personal sphere of an individual, including racial origin, political opinion, religious or spiritual convictions, socioeconomic condition, biomedical or genetic information, sex life and sexual orientation, among others. Sensitive personal data cannot be disclosed without express prior authorization from the data subject.

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to Law No. 8968, the Agency for the Protection of Individual's Data (PRODHAB) is the entity charged with enforcing compliance with the Laws.

The Constitutional Court and local civil courts also have jurisdiction to hear claims alleging violations of the Laws.

REGISTRATION

Under Law 8968, companies that manage databases containing personal information and that distribute, disclose or commercialize such personal information in any manner must register with the Agency.

Entities that manage databases containing personal information for internal purposes do not need to be registered with PRODHAB.

Databases managed by financial institutions subject to control and regulation from the Superintendent of Financial Entities of Costa Rica do not need to be registered with the Agency.

In-house databases are outside the scope of enforcement of the Laws.

DATA PROTECTION OFFICERS

There is no requirement for a data protection officer.

COLLECTION & PROCESSING

Any company may store personal information and manage a database containing it if the following rules are respected:

- When collecting personal information, private companies and/or the government must respect the “sphere of privacy” to which all individuals are entitled
- Such companies must obtain prior, unequivocal, express and valid consent from the owner of the personal information or his or her representative. Such consent must be written (either handwritten or electronic)
- Companies that maintain personal information about others in their databases must ensure that such information is:
    - Materially truthful
    - Complete and
    - Accurate
- Data subjects must be given access to their personal information and are entitled to dispute any erroneous or misleading information about them at any time
- Companies that manage databases containing personal information and that distribute, commercialize or widespread such personal information in any manner, must comply with Law 8968. Particularly, they must comply with the following:
    - Report and register the company and the database with PRODHAB
    - Report the technical measures to secure the database
    - Protect and respect confidentiality of personal information
    - Secure the information contained in the databases
    - Establish a proceeding to review requests filed by data subjects for the amendment of any error or mistakes in the database

TRANSFER

The transfer of personal information is authorized by the Laws if the data subject provides prior, unequivocal, express and valid written consent to the company that manages the database. Such transfers cannot violate the principles and rights granted in the Laws. Also, there are specific limitations regarding cross-border transfers of personal information.

The transfer of personal information from the person responsible for a database to a service supplier, technological intermediary, or entities in the same economic interest group is not considered a transfer of personal information and thus does not need authorization from the data subject. Also, the transfer of public information (which can be generally accessed) does not need authorization from the data subject.

SECURITY

Any company or individual using and / or managing personal information must take all necessary steps (technical and organizational) to guarantee that the information is kept in a secure environment, and must issue an internal protocol indicating all the procedures that shall be followed during the recollection, storage and use of such information.

If security is breached because of improper management or protection, then the responsible company may be held liable, and may be subject to penalties and civil liability for any harm.

BREACH NOTIFICATION

Any entity managing personal data must inform PRODHAB and affected data subjects about any breach of personal information (such as loss, destruction, or misplacement), within five business days after the time of the breach.

The notification to PRODHAB and data subjects must at least include the following information:

- Nature of the breach;
- Personal data compromised by the breach;
- Immediate corrective actions taken by the entity;
- Other preventive and corrective actions that will be taken;
- Contact information to obtain further information.

Failure to provide notice within the required timeframe may result in a potential fine to be enforced by PRODHAB.

ENFORCEMENT

PRODHAB has begun to enforce the obligations established under the Laws. Individuals may file their claims directly with PRODHAB, which may initiate an administrative procedure against the database manager.

In 20122, PRODHAB received more than 272 complaints (the second highest number in history) regarding potential breaches to data protection regulations.

ELECTRONIC MARKETING

General rules of data protection will apply. There is little to no regulation of electronic marketing.

Notwithstanding the above, the Telecommunications Act set the scope and the mechanisms of regulation for telecommunications (including e-marketing), by describing the data subject’s rights, interests and privacy protection policy. Therefore, pursuant to such Act, marketing companies may not advertise via phone nor email unless they obtain prior and express written consent from the data subject. If such companies do not comply with such condition, they might be sanctioned with a fine that can be between 0,025% and 0,5% of the income of the company of the last fiscal year.

ONLINE PRIVACY

There has been little to no regulation in this area. However, the general rules of data protection issued by the Constitutional Court, with respect to the collection and processing of personal information, apply.

KEY CONTACTS

FACIO & CAÑAS
www.fayca.com/

Carlos J. Oreamuno
Partner
Facio & Cañas
T +(506) 2233 9202
coreamuno@fayca.com

Sergio A. Solera
Partner
Facio & Cañas
ssolera@fayca.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CROATIA

Last modified 12 January 2021

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Act on the Implementation of the General Data Protection Regulation (in Croatian as *Zakon o provedbi Opće uredbe o zaštiti podataka*) was enacted in the Croatian Parliament on April 27, 2018 and came into force on May 25, 2018 (the ‘**Act**’).

Also, the Act on Healthcare Data and Information, which came into force on 15 February 2019, regulates rights, obligations and responsibilities of legal and natural persons within the Croatian healthcare system with respect to healthcare data and information and, inter alia, sets out fundamental principles and standards of their collection, processing and protection.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Act refers to all definitions as stated in the GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Croatian Personal Data Protection Agency (in Croatian as *Agencija za zaštitu osobnih podataka*).

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

The Act does not impose any special registration requirements, save for those imposed by the GDPR.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Act does not contain any special requirements related to data protection officers, other than those imposed by the GDPR. AZOP however must be informed on appointment and change of the DPO.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;

- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;

- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

In application of the possibility left to Member States to deviate from the provisions of the GDPR, the Act provides the following obligations with regards to the collection and processing of personal data:

Processing of Genetic Data

The Act forbids any processing of genetic data for the purposes of life insurance calculations and entering into life insurance agreements. Consent given by data subjects does not validate this restriction.

Processing of Biometric Data

Public authorities and private entities may process biometric data only if such processing is defined by law and is necessary for the protection of persons, assets, classified information or professional secrets, provided that the interests of data subjects that contravene such processing do not prevail. Processing of biometric data necessary for fulfilment of international treaties related to identification of data subjects during crossing of state borders is considered as lawful.

Private entities may process biometric data for the purposes of safe identification of users of services, only based on explicit consent given by the users in accordance with the provisions of the GDPR.

Processing of biometric data (eg fingerprints, eye-scans) for the purposes of working time recording or entry/exit of working premises is allowed only on the basis of a legal obligation or if the employer has provided an alternative mechanism for such purposes (e.g. signature list) and the data subjects provided an explicit consent in accordance with the provisions of the GDPR.

Processing of Personal Data through Video Surveillance

Data controllers (or processors) must provide a clear notification to data subjects that premises (or part of it) is under video surveillance. Such notification must be visible while entering the perimeter of surveillance at the latest, and contain the information provided in Article 13 of the GDPR. Also, a clear and understandable photograph (sticker) must be attached to the notification containing:

- a notice that the object is under video surveillance
- information on the data controller, and
- contact details of the data controller for possible complaints

Records of video surveillance may be kept for 6 months, unless a special law or regulation provides a longer period.

In relation to work premises, such premises may be put under video surveillance by the employer only if the conditions under the work safety regulations have been met, and all employees have been notified in advance on the existence of video surveillance. Premises intended for rest, hygiene and changing room may not be put under video surveillance.

In relation to residential buildings, video surveillance may be installed in such buildings under the condition that 2/3 of all owners agree. However, only access to the building’s entrance and exit and common premises (eg stairways) may be put under video surveillance. Video surveillance used for the purposes to control the effectiveness of cleaners and other staff working in residential building is forbidden.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The Act does not contain any special transfer requirements other than those prescribed by the GDPR.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The Act does not contain any special security requirements other than those prescribed by the GDPR.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Act does not contain any special breach notification requirements other than those prescribed by the GDPR.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as

part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The Croatian Personal Data Protection Agency is the enforcement body in Croatia competent for matters related to privacy and personal data. Its decisions may be challenged by initiating administrative litigation at the competent administrative court.

Administrative fines may not be imposed to public authorities and bodies.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Electronic marketing is regulated by the DP Law. A data controller has to inform a data subject in advance on intention to collect and process his/her data for marketing purposes. A data subject can decline to give his / her consent for the respective processing. However, even if a data subject consents to the particular processing for the respective purposes, the processing is allowed only for as long as the data subject does not oppose the same (opt-out provisions are commonly used in consent forms).

The Act does not contain any special electronic marketing requirements other than those prescribed by the GDPR. It sets the consent age limit for offering of information society services to children to 16.

ONLINE PRIVACY

All rules on data protection are applicable to the electronic communication and online privacy as well. AZOP is in charge of control of all online data processing.

Online privacy and cookies are regulated by the Electronic Communications Act ('Official Gazette of the Republic of Croatia', nos. 73/2008, 90/2011, 133/2012, 80/2013, 71/2014 and 72/2017) which has implemented Directive 2002/58/EZ on personal data processing and privacy protection in electronic communications sector.

Usage of electronic communication network for data storage or access to already stored data in terminal data subject equipment is allowed only with a data subject's consent after he / she was clearly and completely informed on the purpose of the data processing (opt-in option).

The Act does not contain any special online privacy requirements other than those prescribed by the GDPR.

KEY CONTACTS

Boris Dvoršćak
Attorney-at-law
Ilej & Partners law firm ltd.
T +385 1 5634 111
boris.dvorscak@ilej-partners.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CUBA

Last modified 16 February 2022

LAW

Cuba does not have its own data protection law.

Cuba regulates data privacy and protection issues, in general, under the following normative:

- Constitution of the Republic of Cuba (2019) .- article 97
- Decree-Law 35/2021 “On Telecommunications, Information and Communication Technologies and the use of the Radioelectric Spectrum”.
- Decree-Law No. 370/2018 “On the Computerization of the Society in Cuba”.
- Decree 360/2019 "On the Security of Information and Communication Technologies and the Defence of National Cyberspace".
- Resolution No. 99/2019 "Regulation for private data networks".
- Others rules:
    - Regulation for the production of computer programs and applications and the evaluation of their quality (2019).
    - System for registration of computer programs and applications (2019).
    - Regulation with the control measures and the types of security tools that are implemented in private data networks (2019).
    - Regulation with the control measures and the types of security tools that are implemented in private data networks (2019).
    - Regulation of the provider of public accommodation and hosting services in the internet environment (2019).
    - Regulation of the provider of public accommodation and hosting services in the internet environment (2019).
    - Information and communication technology security regulation (2019).
    - Methodology for Information Security Management (2019).

DEFINITIONS

Definition of Personal Data

In the regulatory order, the information is approached in a general sense oriented to the preservation of the confidentiality, integrity and availability of the same, and focuses on establishing rules that regulate the management and treatment of information in general, especially related to cybersecurity issues.

Definition of Sensitive Personal Data

Cuban rules do not provide for an express definition of sensitive personal data.

NATIONAL DATA PROTECTION AUTHORITY

Ministry of Communications.

REGISTRATION

No requirements.

DATA PROTECTION OFFICERS

There is no general requirement under binding Cuban rules for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

Generally, entities must obtain prior express consent from data subjects and provide prior notice to the Ministry of Communications to lawfully collect and process personal data. However, data subject consent is not required in certain circumstances provided by Cuba rules.

TRANSFER

Nothing in the Cuba rules is established concerning transfer.

SECURITY

Organisations must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction of, or damage to, personal information. The measures taken must ensure a level of security appropriate to the harm that may result from such unauthorised or unlawful processing, accidental loss, destruction or damage, and appropriate to the nature of the data.

BREACH NOTIFICATION

The Ministry of Communications, in coordination with other authorities, establishes the Program for Strengthening Cybersecurity and coordinates participation in activities required for this purpose and implements its control and inspection.

The Cuba rules introduced a general requirement for the reporting and notification of actual or suspected personal information breaches. Where personal information is leaked, lost or distorted (or if there is a potential for such incidents), organisations must promptly take relevant measures to mitigate any damage and notify the relevant data subjects and report to the relevant government agencies in a timely manner in accordance with relevant provisions.

Mandatory breach notification

All breaches must be reported according to a four-level security scheme.

ENFORCEMENT

The competent authority for the enforcement of Data Protection rules is the Ministry of Communications, in coordination with the Ministry of Interior, Cuban Central Bank, and other authorities.

ELECTRONIC MARKETING

Natural and legal persons that provide goods and services for digital media are obliged to develop a technically safe environment for commercial transactions in which they operate, in accordance with current legislation.

ONLINE PRIVACY

There is nothing established about online privacy, or cookies, or location data.

KEY CONTACTS

Mercatoria

Aldo Alvarez
Director
Mercatoria
T +53 58050722
aalvarez@mercatoria.net

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CURAçAO

Last modified 28 January 2024

LAW

- **National ordinance personal data protection** *(Landsverordening bescherming persoonsgegevens*, National Gazette 2010, Consolidated text no. 84) “(National Ordinance Personal Data Protection”);
- **General Data Protection Regulation** (the “GDPR”) – a regulation of the European Union which became effective on May 25, 2018 – may have implications for a data controller / data processor as the extra-territorial reach of the GDPR is not only relevant to businesses established in the European Union but also to international businesses established in Curaçao which offer goods or services to individuals in the European Union or monitor their behaviour in the European Union.

DEFINITIONS

Definition of Personal Data

National Ordinance Personal Data Protection

According to the Explanatory Memorandum on the National Ordinance Personal Data Protection the term personal data has a broad meaning. This does not only concern data that can identify a person, but concerns any data that can be associated with a particular person; it is foreseeable that under certain circumstances data can be traced to one person through systematic comparison and lengthy investigations. Personal identifiable confidential data is therefore not only limited to home address, email address, telephone number, membership number and/or identity number.

GDPR

Personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Definition of Sensitive Personal Data

National Ordinance Personal Data Protection

A person’s religion or belief, race, political views, health, sexual life as well as personal data concerning membership of a trade union.

GDPR

Data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

NATIONAL DATA PROTECTION AUTHORITY

National Ordinance Personal Data Protection

The Personal Data Protection Committee as referred to in article 42 of the National Ordinance Personal Data Protection.

GDPR

An independent public authority established by a Member state pursuant to article 51 of the GDPR (Article 4(21), GDPR). The authority is responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the EU.

REGISTRATION

National Ordinance Personal Data Protection

No registration required.

GDPR

Article 30 GDPR requires companies to keep an internal electronic registry, which contains the information of all personal data processing activities carried out by the company.

DATA PROTECTION OFFICERS

National Ordinance Personal Data Protection

Pursuant to article 13 of the National Ordinance Personal Data Protection the responsible party shall execute appropriate technical and organizational measures to secure personal data against loss or any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking account of the technical state of the art and the costs of execution, in view of the risks associated with that processing and the nature of the data to be protected. The measures shall be aimed partly at preventing unnecessary gathering and further processing of personal data.

Besides the measures above, the National Ordinance Personal Data Protection does not contain any clauses on any type of registration, filings of documents to any public agency or having a mandatory data protection officer in place.

GDPR

The appointment of a data protection officer under the GDPR is only mandatory in three situations:

- When the organisation is a public authority or body;
- If the core activities require regular and systematic monitoring of data subjects on a large scale; or
- If the core activities involve large scale processing of special categories of personal data and data relating to criminal convictions.

COLLECTION & PROCESSING

National Ordinance Personal Data Protection

Collection: a natural or legal person, public authority, agency or other body which who has control over a person registration.

Processor: a natural or legal person, public authority, agency or other body which who owns all or part of the has equipment in his possession, with which a personal registration of which he is not the holder.

GDPR

Collection: a natural or legal person, public authority, agency or other body that collect personal data and use it for certain purposes, like a website that markets to users based on their online behaviour.

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority.

TRANSFER

National Ordinance Personal Data Protection

Contains no clauses.

GDPR

The GDPR restricts transfers of personal data outside the European Economic Area, or the protection of the GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.

SECURITY

National Ordinance Personal Data Protection

Pursuant to article 13 of the National Ordinance Personal Data Protection the responsible party shall execute appropriate technical and organizational measures to secure personal data against loss or any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking account of the technical state of the art and the costs of execution, in view of the risks associated with that processing and the nature of the data to be protected. The measures shall be aimed partly at preventing unnecessary gathering and further processing of personal data.

GDPR

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (article 32 GDPR).

BREACH NOTIFICATION

National Ordinance Personal Data Protection

Contains no specific clauses.

GDPR

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with article 55 GDPR, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

ENFORCEMENT

National Ordinance Personal Data Protection

Pursuant to article 54 the responsible party who acts in contravention of the provisions of or pursuant to Article 4(3) may be penalized by the Curaçao committee of data protection with a financial penalty in the maximum amount of Naf. 10,000.00 (USD. 5,714.29. 2).

GDPR

The GDPR holds a variety of potential penalties for businesses.

For example, article 77 of GDPR states that:

“Every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating him or her infringes this Regulation.”

Additionally, article 79 of the Regulation states that *“such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence.”*

Penalties

Compensation to Data Subjects. One penalty that may be imposed is compensation to, as stated in article 82 of the Regulation, *“Any person who has suffered material or non-material damage as a result of an infringement of this Regulation”* for the damage they’ve suffered.

Fines

Article 83 of GDPR specifies a number of different fines that may vary based on the nature of the infraction, its severity, and the level of cooperation that “data processors” (i.e. you) provide to the “supervisory authority.” Less severe infringements may incur administrative fines of up to 10,000,000 Euros or 2% of your total worldwide annual turnover for the preceding year (whichever is greater), while more severe infractions may double these fines (20,000,000 or 4% annual turnover).

Individual Member States of the EU may have additional fines and penalties that may be applied as well. However, these additional penalties are not specifically listed in the text of the Regulation since they’re up to the individual EU nations to set— the only guidelines in article 84 of GDPR are that *“Such penalties shall be effective, proportionate and dissuasive”* and that *“Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018.”*

ELECTRONIC MARKETING

National Ordinance Personal Data Protection

N/A.

GDPR

Under article 22 GDPR organizations cannot send marketing emails without active, specific consent.

Companies can only send email marketing to individuals if:

- The individual has specifically consented.
- They are an existing customer who previously bought a similar service or product and were given a simple way to opt out.

ONLINE PRIVACY

National Ordinance Personal Data Protection

Contains no specific clauses.

GDPR

Cookies, insofar as they are used to identify users, qualify as personal data and are therefore subject to the GDPR. Companies do have a right to process their users’ data as long as they receive consent or if they have a legitimate interest.

Location data, the GDPR will apply if the data collector collects the location data from the device and if it can be used to identify a person.

If the data is anonymized such that it cannot be linked to a person, then the GDPR will not apply. However, if the location data is processed with other data related to a user, the device or the user’s behavior, or is used in a manner to single out individuals from others, then it will be “personal data” and fall within the scope of the GDPR even if traditional identifiers such as name, address etc. are not known.

KEY CONTACTS

HBN Law & Tax
hbnlawtax.com/

Maarten Willems
Senior Associate
HBN Law & Tax
T +297 588 6060
maarten.willems@hbnlawtax.com

Misha Bemer
Partner
HBN Law & Tax
T +297 588 6060
misha.bemer@hbnlawtax.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CYPRUS

Last modified 21 February 2022

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Protection of Physical Persons Against the Processing of Personal Data and Free Movement of such Data Law 125(I) /2018, that implements certain provisions of the GDPR into local law, entered into force on July 31, 2018 (the “ **Law**”).

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor " *processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Law uses the definitions provided under the GDPR without any derogation.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The authority designated under the Law as being the local regulatory body for the purposes of the GDPR is the Commissioner for the Protection of Personal Data in Cyprus (the “Commissioner”).

The Law affords certain powers to and imposes obligations on the Commissioner which are in addition to the GDPR, including, inter alia, the following:

- Examination of complaints and providing information to the person making the complaint within 30 days of submission thereto.
- The obligation to inform the data subject, the data controller and the processor of the deadlines indicated under Articles 60-66 of the GDPR.
- The publication of a list of processing activities requiring the appointment of a data protection officer.
- To consult specialists or the police for exercising its regulatory powers under Article 58 of the GDPR.
- To enter, without giving any prior notice to the data controller or the processor or their representatives, any office, business premises or means of transport with the exception of housing premises, for inspections.

- To inform the Attorney General's Office and / or the police for breaches of the GDPR and the national law giving rise to criminal liability.
- To permit the combination of filing systems and to impose terms and conditions in relation thereto.
- To impose terms and conditions to the exemption from the obligation of the data controller to notify data subjects for breaches of personal data as provided for in Article 23 of the GDPR.
- To impose explicit restrictions on the transfer of special categories of personal data to third countries or international organizations.

Further, the Certification Body for the purposes of Article 43 of the GDPR is the Cyprus Organisation of the Promotion of Quality which is the national organization for accreditations in Cyprus operating under the Standardisation, Accreditation and Technical Notification Law (L156(I)/2002).

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

There is no registration applicable with the exception of what is referred to in the immediately succeeding paragraph for data protection officers.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

> According to the Law, the Commissioner may draw up and make available to the public a list of the processing operations and / or other instances which shall deem necessary the designation of a data protection officer (the “ DPO”) by the data controller and the processor. A list of names of data controllers and processors who have designated a DPO may be published on the Commissioner’s website provided the data controller and the processor wish to be included therein.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);

- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Collection and procession of genetic and biometric data for the purpose of health and life insurance is prohibited.

Subject to the above, where processing of genetic and biometric data is based on consent, subsequent and separate consents should be obtained for any further processing.

Further, according to the Law, impact assessment and prior consultation with the Commissioner are required in the following instances:

- when a combination of filing systems of public authorities or certification bodies, is conducted in relation to special categories of personal data or data relating to criminal offences or penalties or will be carried out on the basis of the use of an ID number or any other identifier of general application;
- where, subject to the provisions of Article 23 of the GDPR, measures are taken by the data controller to restrict the rights referred to under Article 12, 18, 19 and 20 of the GDPR;
- where the data controller is exempted from the obligation to notify data subjects for breaches of personal data for one or more of the purposes listed in Article 23(1) of the GDPR, including inter alia, national security, defense, public security, prevention, investigation, detection or prosecution of criminal offences etc;

- where national legislation or regulations issued pursuant thereto provide for a specific action or series of processing activities; and
- where special categories of personal data will be transferred in a third country or an international organization by the controller or the processor, on the basis of a derogation for specific situations provided for under Article 49 of the GDPR.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules and standard contractual clauses. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defense of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

With regards to transfer of special categories of personal data, prior to such data being transferred to a third country or an international organization on the basis of appropriate safeguards provided for under Article 46 of the GDPR or on the basis of binding corporate rules under Article 47 of the GDPR, the data controller or the processor needs to inform the Commissioner of its intention in transferring the said data. The Commissioner may impose express restrictions for such transfer.

Similarly, when special categories of personal data are to be transferred to a third country or an international organization on the basis of a derogation for specific situations provided for under Article 49 of the GDPR, an impact assessment is required to be carried out as well as prior consultation with the Commissioner and the Commissioner may, for important reasons of public interest, impose express restrictions for such transfer.

In light of the Schrems II decision, the European Data Protection Board (EDPB) has issued Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, in respect of transfers made under the standard contractual clauses. The Commissioner directs organisations to the EDPB Recommendations 01/2020 and urges them to follow the guidance of the EDPB.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

There are no derogations or additional requirements introduced by the Law in relation to security.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

According to the Law, the data controller may be exempted, in whole or in part, from his obligation to notify data subjects for breaches of personal data for one or more of the purposes listed in Article 23(1) of the GDPR, including *inter alia*, national security, defense, public security, prevention, investigation, detection or prosecution of criminal offences etc. In order for the foregoing to apply, an impact assessment and a prior consultation with the Commissioner need to be conducted. The Commissioner may also set out specific terms and conditions for such exemption.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

According to the Law, the Council of Ministers may, upon a recommendation of the Commissioner, issue regulatory administrative acts (secondary legislation) in order to effectively enforce the GDPR and applicable national law.

Further, the Law provides that the Commissioner for the Protection of Personal Data shall impose administrative fines in accordance with Article 83 of the GDPR. Further, the Law provides that an administrative fine imposed to a public authority or body, which relates to non-profitable activities shall not exceed EUR 200,000.

The Law provides, inter alia, that breaches of, inter alia, Articles 30, 31, 33, 34, 35, 42 and of Chapter V of the GDPR, shall constitute a criminal offence which may result in the imposition of imprisonment up to three years and / or monetary fine up to EUR 30,000 or imprisonment up to five years and / or monetary fine up to EUR 50,000, depending on the breach.

Where the data controller or processor is a company or a group of undertakings, then the person indicated as such in its article of association will be held liable for breaches of the GDPR and / or the national law. In case of public authorities or bodies, the head of such authority or the person who is effectively exercising the administration of such authority will be held liable for such breaches.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Regulation of Electronic Communications and Postal Services Law of 2004 (112(I)/2004) as amended (the "**Electronic Communications and Postal Services Law**") will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (*eg*, an email address is likely to be personal data for the purposes of the Electronic Communication and Postal Services Law).

Section 106 of the Electronic Communications and Postal Services Law states the following:

1. The use of automatic calling machines, fax, or electronic mail, or SMS messages, for the purposes of direct marketing, may only be allowed in respect to subscribers or users who have given their prior consent

2. Unsolicited communications for the purposes of direct marketing, by means other than those referred to in (1) above, are not allowed without the consent of the subscribers or users concerned

3. The rights referred to in (1) and (2) above shall apply to subscribers who are natural persons. The Commissioner of Electronic Communications and Postal Regulation, may, after consultation with the Personal Data Commissioner, issue orders to safeguard that legitimate interests of legal persons, regarding unsolicited communications, are adequately protected. In 2005, the Commissioner of Electronic Communications and Postal Regulation issued the 2005 Order regarding Safeguarding the Interests of Legal Persons in relation to Unsolicited Communications, by virtue of which the protection from unsolicited communications for the purposes of direct marketing has been extended to legal persons as well

4. Notwithstanding (1) above, in cases where a natural or legal person obtains from its customers contact details for electronic mail, in the context of the sale of a product or a service, the same natural or legal person may use these electronic details for direct marketing of its own similar products or services, provided that customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of their electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use, and

5. Electronic mail sent for direct marketing must not disguise or conceal the identity of the sender or the person on whose behalf and / or for the benefit of the communication is made, or without a valid address to which the recipient may send a request that such communication cease.

ONLINE PRIVACY

Part 14 of the Electronic Communications and Postal Services Law deals with the collection of location and traffic data and use of cookies (and similar technologies) by publically available electronic communication service providers.

Traffic Data

Traffic Data concerning subscribers and users, which are submitted to processing so as to establish communications and which are stored by persons, shall be erased or made anonymous at the end of a call, except:

- for the purpose of subscriber billing and interconnection payments, and

- if the subscriber or user consent that the data may be processed from a person for the purpose of commercial promotion of the services of electronic communications of the latter or for the provision of added value services. Users or subscribers have the possibility to withdraw their consent for the processing of Traffic Data at any time.

The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information. Users or subscribers shall be given the possibility to withdraw their consent for the processing of Traffic Data at any time.

Location Data

Location Data may only be processed when made anonymous, or with the explicit consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.

The service provider must inform the users or subscribers, prior to obtaining their consent, of the following:

- type of Location Data which will be processed
- the purpose and duration of the processing, and
- whether the data will be transmitted to a third party for the purpose of providing the value added service.

Users or subscribers shall be given the possibility to withdraw their consent for the processing of Location Data at any time.

Cookie Compliance

The storage and use of cookies and similar technologies is permitted only if the subscriber or user concerned has been provided with clear and comprehensive information, inter alia, about the purposes of the processing, and has given his consent in accordance with the Processing of Personal Data Law.

The above shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

With regards to information society services, when such services are addressed to a child and provided to him / her on the basis of his / her consent – such consent is valid if he / she is at least 14 years old.

KEY CONTACTS

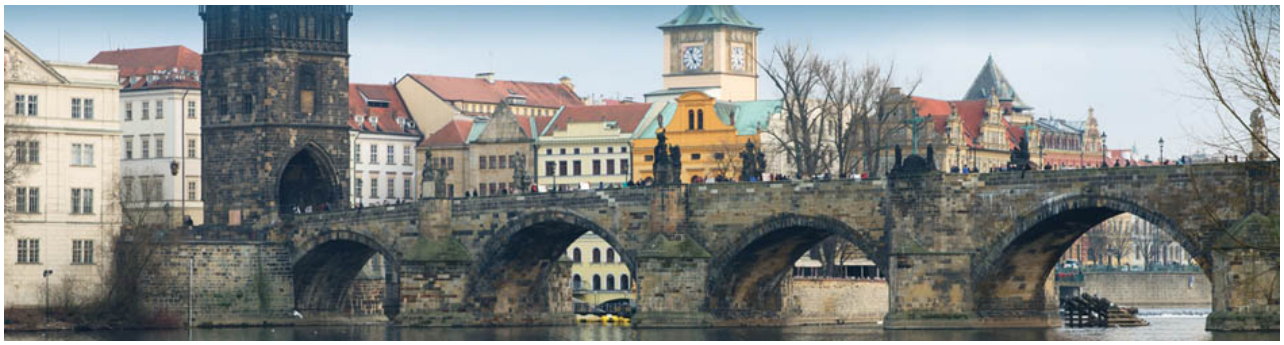
Pamboridis LLC
www.pamboridis.com/

Christy Spyrou
Partner
T +357 22 752525
spyrou@pamboridis.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

CZECH REPUBLIC



Last modified 19 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The new Czech Act No. 110/2019 Coll., on Personal Data Processing, being the Czech GDPR implementation law, finally came into effect on 24th April 2019. This statute fully replaced the older Personal Data Protection Law (Act No. 101 /2000 Coll., as amended) and regulates personal data processing within the scope of Regulation (EU) 2016/679 and then processing of this data by competent authorities for preventing, searching for and detecting criminal activity, ensuring safety and public order etc.

It also regulates jurisdiction of the Office for personal data protection and personal data processing at time of ensuring defense and security of the Czech Republic.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Czech Republic is supervised by the Office for Personal Data Protection (UOOU).

UOOU is the central administrative authority for the protection of personal data, which is in Czech Republic governed by Regulation (EU) 2016/679 and the Act No. 110/2019 Coll.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data

processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organisations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorised by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay, Japan and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules and standard contractual clauses. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

When dealing with e-marketing, it is necessary to bear in mind that it is quite strictly regulated in terms of Act No. 480/2004 Col. on Certain Services of Information Society ("CSIS") as well as other previously mentioned regulations (esp. the Data Protection Directive and the Act) and partially also by the Act No. 127/2005 Coll., on electronic communications (“AOC”), being further described in the Online Privacy section.

CSIS states that before sending an e-mail containing marketing information, the consent of the receiver must be obtained (so called "opt-in" principle). In some cases, such as e-marketing sent to existing customers of the sender, the consent of the customer is implied until it is withdrawn (so called "opt-out" principle). Furthermore, each such message must contain clear and visible information that any further sending of such e-mails can be rejected by the receiver together with the sender's contact information and information on whose behalf the e-mail is being sent. Last but not least, each such e-mail must be clearly tagged as a commercial message.

In order to maintain e-marketing as an effective tool, its sender should operate with good-quality databases, which enable a direct targeting of the relevant message. The sender should ensure, in particular, that:

i. he will duly obtain the right to use the database for e-marketing purposes; and also that
ii. personal data in the database were lawfully obtained and can be lawfully disposed of by the database owner.

When processing personal data for marketing databases, it is necessary to abide strictly by the Act. All rules described above apply to e-marketing respectively.

ONLINE PRIVACY

Online privacy is also supervised by the Office. Handling personal data is subject to the similar rules as mentioned above and specific issues are governed by Act No. 127/2005 Coll. on Electronic Communications (‘**AEC**’).

Consent to collection and processing of personal data may be expressed by electronic means, especially by filling in an electronic form.

Public electronic communication service providers are obliged to ensure the security of the personal data they process which includes technical security and creation of internal organisational regulations.

In cases of a personal data breach a public electronic communication service provider is obliged to notify the Office "*without necessary delay*", and in the event that the breach of protection could very significantly affect the privacy of a certain individual, such person must be notified as well.

Apart from a few exceptions, traffic data held by a public electronic communication service provider must be erased or anonymised when it is no longer necessary for the transmission of a communication.

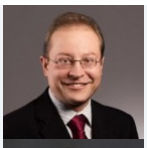
As regards cookies, the Czech law is since 1 January 2022 using the ‘opt-in’ principle (by amending the Section 89 (3) of the Czech Electronic Communications Act), now finally being in line with other EU countries, as opt-in was introduced by Directive 2009/136/EC.

Relevant supervising and enforcing authorities in this area are primarily the Office and to some extent also the Czech Telecommunication Office.

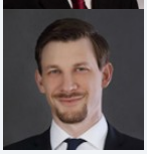
KEY CONTACTS

Tomáš Ščerba
Partner
DLA Piper Prague LLP
T +420 222 817 760
tomas.scerba@dlapiper.com

Jan Rataj



Senior Associate
T +420 222 817 800
jan.rataj@dlapiper.com



Jan Metelka
Associate
T +420 222 817 825
jan.metelka@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

DEMOCRATIC REPUBLIC OF CONGO

Last modified 23 February 2024

LAW

The protection of personal data is included in the law establishing the digital code N°23-010 of 13 March 2023 and published in the official journal on 11 April 2023 (the “**Digital Code Law**” or “**Digital Code**”). The Digital Code Law entered into force on the date of its approval (13 March 2023). Several implementing decrees referred to in the Digital Code Law have not yet been issued.

DEFINITIONS

Definition of Personal Data

Personal data is defined in Article 183 of the Digital Code Law and listed in eight different categories:

1. **Personal identification data, in particular**: first name, surname, middle name, date and place of birth, age, marital status, national identification number, valid official identity document or any other biometric data, in particular photographs, sound recordings, images, fingerprints and iris scans;
2. **Correspondence data**: telephone numbers, physical, postal and e-mail addresses;
3. **Professional data**: status, job held, employer, remuneration;
4. **Billing and payment data**: invoice amounts and history, payment status, reminders, payment balances, direct debit date;
5. **Bank details**: bank code, account and credit card number, bank name / address / contact details, transaction references;
6. **Data on legal entities** under public or private law showing personal data;
7. **Data on family circumstances**; and
8. **Data concerning court decisions**.

Definition of Sensitive Personal Data

There is no separate definition of sensitive data, but the Digital Code prohibits, as a matter of principle, the processing of certain data which can be considered as sensitive, such as personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, the status of refugees or stateless persons, trade union membership, sex life or, more generally, data relating to the state of health.

For the purposes of this definition, “processing” is to be understood as the operation or set of operations which is performed upon personal data, whether by means of wholly or partly automated processes, such as collection, recording, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

There are several exceptions to this principle stated in the Digital Code. The processing of such data will be admissible should, for instance, one consents to such processing for a well determined purpose. The processing of such data for statistical analysis or health reasons will usually, and within the boundaries of the Law, be equally accepted.

NATIONAL DATA PROTECTION AUTHORITY

APD (*Autorité de Protection des Données*) or the authority in charge of data protection.

According to Article 262 of the Digital Code provides that a decree from the Prime Minister will have to establish the APD and determine its organization, its functioning and regulatory powers. To date, no such decree has been adopted.

REGISTRATION

The Digital Code provides for a declaration regime and an authorisation regime with the APD (*Autorité de Protection des Données*).

The declaration regime is applicable to all actors processing data and such declaration is to be performed by the person or entity responsible for the processing of personal data.

The authorisation regime is applicable for the processing of certain (more sensitive) data, such as the processing of national identification numbers, genetic data, data regarding criminal records, etc. or whenever personal data will be transferred to a third country.

Considering that the APD has not yet been established, the declaration and authorisation regimes are not yet in practice complied with.

DATA PROTECTION OFFICERS

The Digital Code provides for the possibility to designate a "*délégué à la protection des données à caractère personnelles*", which is a person responsible for the protection of personal data or Data Protection Officer, without however regulating such role in detail. The Digital Code only provides for some of its duties, namely:

1. to inform and advise the controller or processor and the employees who carry out the processing on their obligations under the data protection provisions of the Digital Code;
2. monitoring compliance with the data protection provisions of the Digital Code and with the controller's or processor's internal rules on the protection of personal data, including with regard to the allocation of responsibilities, the awareness and training of staff involved in processing operations, and related audits;
3. providing advice, on request, on data protection impact assessments and verifying that they are carried out in accordance with the Digital Code;
4. cooperating with the APD;
5. acting as a focal point for the authority responsible for the protection of personal data on matters.

COLLECTION & PROCESSING

As a matter of principle, the collection and processing of personal data (whether sensitive or not) is prohibited. It can be carried out with the prior and explicit consent of the person concerned or on the request of the public prosecutor's office, provided that the consent of the person concerned can always be proven. One’s consent can be withdrawn at all times.

TRANSFER

The Digital Code distinguishes between the transmission and transfer of personal data.

The transmission of personal data, which refers to the transmission of personal data between persons responsible of transmitting personal data (without these being Data Protection Officers) whether private or public entities, is legal and permitted provided the person whose personal data are being transmitted granted his / her explicit and prior consent.

The transfer of personal data refers to the transfer of data to another country or a data service provider whose servers are located in another country. Such transfer is legal and accepted provided that the third country or international organization where the date will be effectively kept provides a level of security and protection equal or better as the level of security and protection provided by the Digital Code.

SECURITY

Not applicable.

BREACH NOTIFICATION

The person responsible for the data protection or Data Protection Officer, if one was designated, must notify the APD without delay of any personal data breach that has affected one’s personal data.

Any person who considers that his / her personal data have been misused or used without consent shall have the right to lodge a complaint with the APD. The APD shall inform the person lodging the complaint of the progress and outcome of the complaint, including the possibility of judicial remedy.

It is unclear at this stage how a notification must be performed as the decree organising the APD has not yet been drafted nor adopted.

Mandatory breach notification

Not Applicable.

ENFORCEMENT

No known cases as the Law is relatively new.

Administrative sanctions may apply and decided by the APD. Fines range from USD 3,000 to USD 70,000 for the entity that breached the Digital Code.

ELECTRONIC MARKETING

Not applicable.

ONLINE PRIVACY

Not applicable.

KEY CONTACTS

PKM Africa
www.lawpkm.com/

Yves Brosens
Partner
PKM Africa
T +32 472 582 000
yves.brosens@lawpkmafrica.com

Pierre Vanholsbeke
Junior Partner
PKM Africa

T + 32 472 79 54 24
pierre.vanholsbeke@lawpkmafrica.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

DENMARK

Last modified 19 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

To implement the GDPR, the Danish Parliament enacted the Danish Act on Data Protection (the 'Danish Data Protection Act’) on May 17, 2018, enforceable on May 25, 2018 and replacing the previous Danish Act on Processing of Personal Data (Act no. 429 of 31/05/2000). Hence, data protection and processing in Denmark is now regulated by the GDPR as supplemented by the Danish Data Protection Act.

The Danish Data Protection Act does not apply to Greenland and the Faroe Islands.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions used in the Danish Data Protection Act correspond to the definitions as set out in the GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the CNIL in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party), also known as the “EDPB”, is comprised of delegates from the national supervisory authorities and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T +45 33 19 32 00
dt@datatilsynet.dk

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or

processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

In Denmark, the following types of processing require the DPA’s preapproval:

- private data controllers’ processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (‘Special Categories of Personal Data’), solely in the public’s interest
- disclosure of personal data as mentioned in Articles 9(1) and 10 of the GDPR, originally processed for the sole purpose of carrying out scientific or statistic studies, if i) such data is to be processed outside the geographical scope of the GDPR, ii) the data constitutes biological material or iii) if the data is to be published in a recognised scientific journal or similar
- processing personal data in a register on behalf of a private data controller:
  - solely for the purpose of warning other businesses from engaging in business with or employing a natural person
  - with the intention of commercial exploitation of data on the natural person’s creditworthiness and financial solidity, or
  - for the creation of a register on judicial information

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

Under the Regulation, organizations shall designate a data protection officer (‘DPO’) in any case where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity
- the core activities of the data controller or the processor consist of processing operations which, by their nature, their scope and / or their purposes, require regular and systematic monitoring of data subjects on a large scale, or
- the core activities of the controller or the processor consist of processing on a large scale of Special Categories of Personal Data and personal data relating to criminal convictions and offences

The DPO shall be selected based on professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in the GDPR.

Under the Danish Data Protection Act, the DPO is subject to a duty of secrecy and is prohibited from wrongful disclosure or use of any personal data processed in their capacity of being DPO.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise, or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation, that is to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider when assessing whether the new process is compatible with the purposes for which the personal data was initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose;
- the context in which the data have been collected;
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible);
- the possible consequences of the new processing for the data subjects;
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data is used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible privacy notices should therefore be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are made based on grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The GDPR differentiates between 1) Personal data, 2) Special Categories of Personal Data, 3) Data on criminal offences and 4) National identification numbers (CPR numbers). See below.

1. Personal data

Under the GDPR, data controllers may legally register and process personal data (all data except the Special Categories of Personal Data, Data on criminal offences and national identification numbers) only when at least one of the following conditions are met:

- the data subject has given his explicit consent in accordance with article 7 and 8 (children’s consent) of the GDPR;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or any other natural person;
- processing is necessary for the performance of a task carried out in the public interest or for the performance of a task carried out in the exercise of official authority vested in the data controller; or
- processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third-party to whom the data is disclosed, unless these interests are overridden by either the data subject’s fundamental rights including its civil rights or other interests of the data subject.

2. Special Categories of Personal Data

Special Categories of Personal Data (as detailed under 'Registration') may be processed only when at least one of the following conditions are met:

- the data subject has given his explicit consent to the processing of such data for one or several purposes;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment law;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the person concerned is physically or legally incapable of giving his or her consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment, or the management of medical and health care services, and where those data are processed by a health professional subject under law to the obligation of professional secrecy;
- processing is necessary for reasons of substantial public interest. The DPA must approve the processing unless such is carried out by a public organization.

Personal data and Special Categories of Personal Data may be processed, if such process is carried out in relation to the data subject’s employment at the data controller, if such process is necessary for the data controller to comply with employment-related obligations or rights under applicable law or collective agreements, or if the process is necessary for the data controller or third-party’s possibility to pursue legitimate interests originating from other legislation or collective agreements as long as the civil rights and interests of the data subject precedes.

Furthermore, personal data may be processed where the processing takes place for the sole purpose of carrying out statistical or scientific studies of significant importance to society and where such processing is necessary in order to carry out these studies. Sharing of personal data for such purposes will, however, be subject to the conditions set forth in the Danish Ministerial Order no. 1509 of 18 December 2019, according to which personal data shared for the purpose of carrying out statistical or scientific studies must, amongst other, be pseudonymised before sharing, unless direct identifications is strictly necessary.

3. Data relating to criminal convictions and offences

Data relating to criminal convictions and offences may be processed by public data controllers only if the processing is strictly necessary for the performance of regulatory and public tasks. No such data can, however, be disclosed, unless at least any of the following conditions are met:

- the data subject has given explicit consent to such disclosure;
- disclosure takes place for the purpose of safeguarding private or public interests which clearly override the interests of secrecy, including the interests of the person to whom the data relate;
- disclosure is necessary for the performance of the activities of an authority or required for a decision to be made by that authority; or
- disclosure is necessary for the performance of tasks for a public authority by a person or an enterprise.

Private data controllers may process data relating to criminal convictions and offences, if the data subject in question has given his or her explicit consent in accordance with article 7 of the GDPR, or if the processing is strictly necessary to carry out interests significantly exceeding the interests of the data subject. None of the data may be disclosed without the explicit consent of the data subject, unless such disclosure takes place for the purpose of safeguarding public or private interests, including the interests of the person concerned, which clearly override the interests of secrecy.

Both public and private actors may process personal data about criminal convictions and offences if at least one the following conditions are met:

- processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment law;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the person concerned is physically or legally incapable of giving his or her consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
- the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment, or the management of medical and health care services, and where those data are processed by a health professional subject under law to the obligation of professional secrecy; or
- processing is necessary for reasons of substantial public interest. The DPA must approve the processing unless such is carried out by the public organization.

4. National identification numbers

National identification numbers (in Danish ‘*CPR-nummer*.’) may be processed by public organizations for the purpose of identification or as reference number.

Private data controllers may process *CPR-nummer* when at least one of the following conditions are met:

- the process is required under statutory law;
- the data subject concerned has given his or her explicit consent in accordance with article 7 of the GDPR;
- the processing is carried out for scientific or statistic purposes (however not for publication which requires a specific consent);
- the CPR-nummer disclosed as part of the company’s natural operations and such disclosure is of significant importance to the company to ensure identification of the data subject in question or requested by a public authority;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment law;

- processing is necessary to protect the vital interests of the data subject or of another natural person where the person concerned is physically or legally incapable of giving his or her consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
- the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment, or the management of medical and health care services, and where those data are processed by a health professional subject under law to the obligation of professional secrecy; or
- processing is necessary for reasons of substantial public interest. The DPA must approve the processing unless it is carried out by a public data controller.

5. Transparency requirements

The data controller must, at the time when personal data are obtained (no later than within one month after), provide the data subject with the necessary information to fulfil the duty of information, including information about:

- the identity of the data controller, his representative and the DPO (if applicable);
- the contact details of the data controller / the representative;
- the categories of data concerned;
- the purposes of the processing for which the data is intended as well as the legal basis for the processing;
- the legitimate interests pursued by the data controller, where the processing is based on article 6(1)(f) of GDPR;
- the recipients or categories of recipients of the personal data, (if any);
- (where applicable), information of transfer of data to third countries or international organizations or the intention hereof, as well as reference to the appropriate and suitable safeguards in connection with such transfers;
- The period for which the data will be stored;
- The data subject’s right to withdraw a consent at any time;
- The data subject’s rights, including to lodge a complaint, deletion, insight and correction;
- From which source the personal data originate (if applicable), and whether it came from publicly accessible sources (if applicable);
- The existence of automated decision making (if applicable).

Under the Danish Data Protection Act the above-mentioned obligations do not apply if interests of the public, other people, or the data subject itself, exceed the data subject’s interest in obtaining the information.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of

appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available, and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject. Notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The Danish Data Protection Act does not regulate transfer of personal data. Thus, the article of the GDPR applies, under which data controllers may transfer all types of personal data to a third country or an international organization out of the EU/EEA if any of the following conditions are met:

- the EU Commission has established that the third-country / area or one or more specific sectors in the third country, or the international organization has adequate safeguards with respect to the protection of the rights of the data subject;
- the controller or processor has provided appropriate safeguards, on the condition that enforceable data subject rights and effective legal remedies for data subjects are available (such as through binding corporate rules – approved by the DPA);
- the data controller or data processor and the international organization enter into the standard terms approved by the EU Commission.

If no approval has been obtained on the third country’s adequate safeguards and no appropriate safeguards have been provided including binding corporate rules, personal data can be transferred to a third country or an international organization if one of the following criteria are met:

- the data subject has given his explicit consent;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject’s request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;
- the transfer is necessary or legally required on important public interest grounds;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or other natural person, where the person concerned is physically or legally incapable of giving his or her consent;

- the transfer is made from a register which according to law or regulations is open to consultation either by the public in general or by any person who can demonstrate legitimate interests, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However, the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The Danish Data Protection Act does not set out provisions on security requirements. Thus, the articles of the GDPR apply, under which data controllers and data processors must implement appropriate technical and organizational security measures necessary to protect data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in the Danish Data Protection Act.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Danish Data Protection Act does not set out provisions on notification in case of security breach. Thus, the articles of the GDPR apply, under which the data must notify the DPA no later than 72 hours after becoming aware of the security breach.

Breaches can be reported to the Danish Data Protection Agency by filling out a form on the Danish Business Authority’s website.

Further, if the security breach is likely to expose the data subject to risk related to its rights and civil rights, the data controller shall notify the data subject without unnecessary delay.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR provides specific provisions for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" because of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The DPA is responsible for the supervision of all processing operations covered by the Danish Data Protection Act.

The DPA can request any information provided necessary for the DPA’s operations including decision-making on whether the Danish Data Protection Act and the GDPR apply or not.

The DPA and its personnel can without a court order request access to premises from which processing of personal data is performed.

The DPA’s decisions are final and not subject to recourse.

The DPA may investigate data processing occurring in Denmark and the legality thereof, despite the processing being subject to foreign law.

The DPA may publish its findings and decisions.

Any person suffering material or nonmaterial damage due to non-legal data processing can claim damages.

Unless a higher penalty is impeded, processing deemed unlawful under the Danish Data Protection Act, is sanctioned with a fine or prison for up to six months.

In general, the GDPR aims to sanction with fines which are effective, reasonable and have preventive effect. More specific, certain violations can be sanctioned with a fine of a maximum of EUR 10,000,000 or 2% of the total annual turnover (if a company). Other types of violations can be sanctioned with a fine of a maximum of EUR 20,000,000 or 4% of the total annual turnover (if a company).

The statute of limitation period is five years.

ELECTRONIC MARKETING

The GDPR applies to most electronic marketing activities, as these involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

In general, unsolicited electronic marketing requires prior opt-in consent. The opt-in requirement is waived under the ‘ same service / product’ exemption. The exemption concerns marketing emails related to the same products / services as previously purchased from the sender by the user provided that:

- the user has been informed of the right to opt out prior to the first marketing email;
- the user did not opt out; and
- the user is informed of the right to opt out of any marketing email received. The exemption applies to electronic communication such as electronic text messages and email but does not apply with respect to communications sent by fax.

Direct marketing emails must not disguise or conceal the identity of the sender.

The GDPR applies to electronic marketing activities involving usage of personal data (e.g. an email address which includes the recipient's name).

Under the GDPR companies are prohibited from disclosing personal data to another company for direct marketing purposes or use the data on behalf of a company for marketing purposes, unless the data subject has given his or her explicit consent. In this regard, the strict standard for consent under the GDPR must be noted, and marketing consent forms must include a clearly worded opt-in mechanism (such as a ticking of an unticked consent box, or the signing of a statement, and not merely an acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

General customer information (general information forming the basis for customer classification) may, however, be disclosed and processed without the data subject’s consent, if such is necessary for the purposes of legitimate interests pursued by the company and these interests are not overridden by the interests of the consumer. However, Special Categories of Personal Data and CPR-numbers can only be processed for marketing purposes by the consent of the data subject.

The company disclosing the personal data or processing the personal data on behalf of a company for marketing purposes, must prior hereto ensure that the data subject has not declined receiving marketing material by registering as such in the Danish Central Office of Personal Registration.

Particularly for controllers selling catalogues of data on natural persons or addressing these natural persons on behalf of a company it applies that only the natural person’s name, work position, address, occupation, email, phone- and fax number and business information published in business registers can be processed. Any other kind of data can only be processed if the data subject has consented thereto.

Further, specific rules on electronic marketing (including circumstances in which consent must be obtained) are regulated in Directive 2009/136/EC (the ePrivacy Directive), as transposed into the local laws of each Member State. In Denmark, the ePrivacy Directive has among other things been implemented in the Danish Marketing Practices Act.

Under the Danish Marketing Practices Act, a trader must not approach anyone by means of electronic mail, an automated calling system or a facsimile machine (fax) for the purposes of direct marketing unless the natural person concerned has given his prior consent. The trader must allow free and easy revocation of the consent.

Notwithstanding the above, a trader that has received a customer's electronic contact details in connection with the sale of products may market similar products to that customer by electronic mail, provided that the trader has clearly and distinctly given the customer the opportunity, free of charge and in an easy manner, of declining this both when giving his contact details to the trader and in all subsequent communications.

The ePrivacy Directive is to be replaced by the ePrivacy Regulation, a change which was forecast for spring 2018, however, now postponed indefinitely. From the wording of the latest draft, we can expect a significant toughening of the online and direct marketing landscape and, predictably, a convergence with the provisions in the GDPR.

ONLINE PRIVACY

Traffic data

Traffic data qualifies as personal data. Providers of telecommunication services may collect and use the following traffic data to the following extent:

- the number or other identification of the lines in question or of the terminal;
- authorization codes, additionally the card number when customer cards are used;
- location data when mobile handsets are used;
- the beginning and end of the connection, indicated by date and time and, where relevant to the charges, the volume of data transmitted;
- the telecommunications service used by the user;
- the termination points of fixed connections, the beginning and end of their use, indicated by date and time and, where relevant to the charges, the volume of data transmitted; and
- any other traffic data required for setup and maintenance of the telecommunications connection and for billing purposes.

Stored traffic data may be used after the termination of a connection only where required to set up a further connection, for billing purposes or where the user has requested a connection overview.

The service provider may collect and use the customer data and traffic data of subscribers and users to detect, locate, and eliminate faults and malfunctions in telecommunications systems. This applies also to faults that can lead to a limitation of availability of information and communications systems or that can lead to an unauthorized access of telecommunications and data processing systems of the users.

Otherwise, traffic data must be erased by the service provider without undue delay following termination of the connection.

Service providers must inform the users immediately, if any faults of data procession systems of the users become known. Furthermore, the service provider must inform the users about measures for detecting and rectifying faults.

Location Data

Location Data qualifies as personal data. This data may only be processed as required for the provision of requested services and is subject to prior information of the user. For all other purposes, the user’s informed consent must be obtained. According to Section 4a BDSG, 13 German Telemedia Act (TMG) this means that:

- the user’s consent must be intentional, informed, and clear. For this purpose, the user must be informed on the type, the scope, the location and the purpose of data collection, processing and use including any forwarding of data to third parties;
- the user’s consent must be recorded properly;
- the user must be able to access the content of his consent declaration any time. It is sufficient that such information is provided upon the user's request;
- the user’s consent must be revocable at all times with effect for the future.

Users must always be informed of the use of cookies in a privacy notice. Cookies may generally be used if they are required to perform the services requested by the user. Otherwise, users must be provided with an opt-out mechanism. For this purpose, information about the use of cookies together with a link about how to adjust browser settings to prevent future use are sufficient.

Germany has not yet taken any measures to implement the e-privacy directive. However, in February 2014 the German Federal Ministry of Economic declared that the European Commission considers the Cookie Directive as implemented in Germany. However, since the European Commission´s exact interpretation is not known, a final official clarification is awaited. It therefore remains to be seen whether an active opt-in, e.g., by clicking on a pop-up screen will be required in the future.

Different rules apply in the case of tracking technologies which collect and store a user’s IP address. Since IP addresses qualify as personal data, their processing for tracking and marketing services requires active opt-in consent.

Directive 2009/136/EC (the ePrivacy Directive) was among other things also implemented in the Danish Act on Electronic Communications Services and Networks which came into force on May 25, 2011 in accordance with the implementation deadline in the Directive. In accordance with this act, the Danish Parliament adopted the Danish Executive Order on Electronic Communications Services and Networks which came into force on May 25, 2018 (the ‘Cookie Order’).

The Cookie Order should be read in the light of GDPR, where the rules regulate collection of data in a broader sense, not considering whether such information may be used to identify a natural person.

Under the “Cookie Order” the use of cookies requires a consent. The consent must be freely given and specific. However, this does not imply that consent must be obtained each time a cookie is used but a user must be given an option. Furthermore, the consent must be informed which implies that a user must receive information about the consequences of consenting. To meet the information requirement, one must:

- Provide the information in a clear and explicit language, that is easy to understand or a similar imagery that is easy to understand, e.g. pictograms;
- Explain the purpose of using cookies;
- Tell the users who is behind the cookies used – this may be the website owner or a third party;
- Inform the user how to give consent or reject the use of cookies;
- Explain how the user can withdraw his or her consent;
- State the duration of the cookies (expiry date).

Finally, the consent must be a clear indication of the user’s wishes, which entails meeting the following requirements:

- The user must be able to consent or refuse to consent to the use of cookies;
- The user must be able to withdraw a previously given consent;
- The user should easily be able to find further information about the use of cookies on the website;

- The consent must be linked to the purpose for which the data collection is to be used.

Previously, the use of a homepage after having received relevant information could (to some extent) be considered to be a valid consent in Denmark. This is no longer the case and now a more explicit consent is required (e.g. the clicking of an “accept” button).

The ePrivacy Directive is to be replaced by the ePrivacy Regulation, a change which was forecast for spring 2018, however, now postponed indefinitely and the timeframe for changes to abovementioned rules are thus currently unknown.

From the wording of the latest draft, however, it is unsurprisingly safe to say that the definition of consent used in the GDPR is carried on and is to be read across into the draft e-Privacy Regulation text. Further, the draft also introduces significant practical changes, so that obtaining consent will require much more effort. Technology providers are required to include default settings which must all be set to preclude third parties from storing information on, or using information about, an end-user’s device. So, browsers would have to be pre-configured so that cookies used for frequency capping of ads or ad-serving would be blocked by default unless a user opts to enable them.

Current position

There has not been changes in the Danish data protection legislation. The Danish supervisory authority (the Danish Data Protection Agency) has had several focus areas for 2023 including child protection, TV surveillance, processing of personal data in pan-European information systems, etc.

With effect from 1 January 2023, an amendment has been made to the executive order on disclosure for research and statistical purposes, which specifies the conditions for disclosure of personal data from statistical or scientific studies under section 10 of the Danish Data Protection Act. In this connection, the rules for erasure of personal data at the end of research projects have been clarified. This has been done to clarify that the data controller may have a legitimate need to process data for a period after the end of the study - e.g. for the purpose of addressing allegations of scientific misconduct. This is because controllers will often be subject to requirements to prove, for a period after the end of their study, that the study is not based on false information or that other researchers must be able to recreate the results. Controllers should consider whether the purpose of processing personal data after the end of the study can be achieved by processing the data in another – e.g. anonymized – form, in accordance with the fundamental data protection law principle of data minimization.

In relation to the right of access regarding children, the Danish Data Protection Agency has stated that the right of access (Article 15) is a personal right that belongs to the individual data subject. This also applies in the case of a child. The child is an independent rights holder. Parents can support their child in exercising the child's right of access by requesting access on behalf of the child. As a rule, each parent can make such a request without documentation of consent from the other parent.

The Danish Data Protection Agency has published various new guidelines, practices and statements including among others:

- guidelines about data processing in connection with direct marketing. This is because direct marketing is one of the most widespread forms of marketing and because direct marketing almost always involves the processing of personal data;
- guidelines about the different GDPR roles in research projects, e.g. the different roles that may apply in clinical research, the role of Ph.D. students, collaboration between public authorities, hospitals, and private actors etc;
- guidelines about public authorities’ use of Artificial Intelligence (AI);
- three guidelines on CCTV surveillance for private organisations, public authorities, and housing organizations. The guidelines go through relevant rules to be aware of when processing and disclosing personal data related to CCTV surveillance, especially related to crime prevention;
- two fundamental decisions regarding the use of cookie walls. Following these decisions, the Danish Data Protection Agency has prepared some general guidelines on the use of cookie walls that companies should use and introduces four conditions to place cookie walls: 1) it must be a reasonable alternative to consent, 2) the

price must be fair, 3) cookie walls must respect the purpose limitation principle, and 4) processing may start after payment has been received;

- a catalogue of security measures (*Katalog over foranstaltninger* (datatilsynet.dk)), which includes a list of organisational and technical measures and descriptions and examples about how to use and implement the measures to mitigate, reduce, or eliminate certain risks. The measures are based on experiences from audits in the private and public sector, data security breach cases, EDPB guidelines, ISO 27001, and ISO 27002;
- guidelines about user and access rights to it-systems, physical locations etc.

Further, at the annual meeting of the Nordic supervisory authorities (Denmark, Faroe Islands, Finland, Iceland, Norway, Sweden, and Åland), the "*Reykjavik Declaration*" was adopted: Reykjavik Declaration.pdf (datatilsynet.dk). One of the goals of the Reykjavik Declaration is to continue to explore the possibilities for a more data- and risk-based process in the selection of where to carry out supervision. In this context, the countries also agreed to work towards greater knowledge-sharing at the European level.

KEY CONTACTS

Marlene Winther Plas
Partner
T +45 33 34 00 47
marlene.plas@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

DOMINICAN REPUBLIC

Last modified 28 January 2024

LAW

Section 44 of the Dominican Constitution recognizes citizens’ right to access their personal data stored in public or private databases, as well as their right to information concerning the purpose and use of the same.

The Constitution also establishes that the processing of personal data must be carried out in accordance to the principles of:

- Reliability
- Legality
- Integrity
- Security, and
- Purpose of the information

The collection, storage and safekeeping of personal data, as well as usage and access rights concerning such personal data, are governed by the provisions of Law No. 172-13 on the Protection of Personal Data enacted December 13, 2013 (DPL).

In addition to setting forth the legal regime for the protection of personal data, the DPL establishes regulations governing the constitution and operation of credit bureaus.

For the purposes of the DPL, the term '*credit bureau*' refers to companies dedicated to collecting, organizing, storing, conserving, providing, transferring or transmitting data regarding consumers (including goods and services related to the same), as well as any other information provided by the Superintendent of Banks.

Law No. 53-07 on High Technology Crimes and Offenses does not specifically refer to personal data but ensures the protection of information systems and their components, as well as the information or data that are stored or transmitted through them, and it also establishes the penalties for crimes committed against them or any of their components or those committed using such technologies to the detriment of individuals or legal entities.

DEFINITIONS

Definition of personal data

Personal data consists of any information, whether numerical, alphabetical, graphic, photographic, or acoustic, or any other type of data which concerns individuals that are identified or identifiable.

Definition of sensitive personal data

The term 'sensitive data' refers to personal data that reveals its subject´s:

- Political opinions

- Religious, philosophical or moral convictions
- Racial or ethnic origin
- Affiliation to labor unions or trade union membership, and
- Information concerning health or sex life

Personal data concerning the health of an individual encompasses any information concerning their past, present or future physical or mental health.

Affected or interested party

Any natural person whose information is the object of data processing, as well as any creditor, whether a natural or legal person, who has or has had a commercial or contractual relationship with a natural person for the exchange of goods and services, where the natural person is the creditor's debtor. As well as any natural or legal person who has had, has or requests to have a good or service of an economic, financial, banking, commercial, industrial, or any other nature, with a financial intermediation institution or with an economic agent.

Data processing

Systematic operations and procedures that allow the collection, conservation, ordering, storage, modification, relation, evaluation, blocking, destruction and, in general, the processing of personal data, as well as its transfer to third parties through communications, consultations, interconnections or transfers.

Data Processor

The natural or legal person, public or private, who carries out the processing of personal data on behalf of the controller.

NATIONAL DATA PROTECTION AUTHORITY

The Dominican Republic does not have a national data protection authority dedicated to overseeing matters related to data protection concerning processing activities performed by private persons or entities.

However, Section 29 of the DPL establishes that databases and registries, whether public or private, intended to provide credit reports (ie credit bureaus) are subject to the inspection and supervision of the Superintendent of Banks.

Additionally, the General Law for the Protection of Consumer or User Rights No. 358-05 determines that the National Institute for the Protection of Consumer Rights, "Pro Consumidor" is the competent authority for monitoring compliance in data protection in consumer matters. The "Pro-Consumidor" cannot impose fines or administrative sanctions but users, consumers and suppliers can initiate conciliation and arbitration processes before them.

REGISTRATION

Except for credit bureaus, the Dominican Republic does not maintain a registration of personal data controllers or databases, nor of companies that carry out the processing of personal data.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer under the DPL.

COLLECTION & PROCESSING

The general rule for the treatment of personal data under the DPL is that consent to process is a requirement. Consent is valid when there is a manifestation of free will, in an unequivocal, specific and informed manner, whereby the data subject consents to the treatment of personal data concerning him or her.

The DPL provides that the treatment and transfer of personal data is illegal when the data has not consented to such usage, unless an exception is provided by law.

For purposes of the foregoing, the DPL defines treatment as operations and procedures (electronic or otherwise), that allow for the:

- Collection
- Storage
- Organization
- Modification
- Evaluation
- Destruction
- In general, the processing of personal data, or
- Its transfer to third parties via communications, interconnections or transfers

Exceptions to the requirement to obtain consent include, among others:

- When the data is obtained from a public source
- When the data is obtained for the exercise of public duties or pursuant to a legal obligation to do so
- When the data is obtained for marketing purposes and is limited to certain basic information (*eg*, name, ID, passport, tax ID)
- The data derives from a commercial, employment or contractual relationship, or from a professional or scientific relationship with the data subject, and is necessary for its development or compliance

TRANSFER

Transfer is considered a form of 'treatment' of personal data under the DPL; hence, the rules apply, including consent requirements. Additional restrictions are provided under the DPL for international data transfers.

Personal data may only be transferred internationally if the owner of the data expressly authorizes such transfer, or if such transfer is necessary for the performance of a contract between the owner of the data and the person or entity responsible for the treatment of the personal data.

SECURITY

The controller and, if applicable, the processor, is required to adopt and implement the necessary technical, organizational and security measures to safeguard personal data and avoid its:

- Alteration
- Loss
- Treatment
- Consultation, or
- Unauthorized access

The DPL prohibits the storage of personal data in files, records or databases that do not meet the necessary technical conditions for guaranteeing their integrity and security. Additionally, credit bureaus and users or subscribers shall take the necessary measures to prevent the alteration, loss or unauthorized access to personal data.

BREACH NOTIFICATION

There is no obligation to provide notice of a breach.

ENFORCEMENT

Since there is no special data protection authority in the Dominican Republic, data subjects have the right to institute *habeas data* proceedings to obtain information about the data held that refers to the relevant data subject.

The DPL expressly recognizes the right of data subjects to recover damages for violations of their right to privacy and the integrity of their personal data. Additionally, the DPL provides criminal sanctions (including fines and imprisonment ranging from six months to two years) which may result from violating the DPL.

Law No. 310-14 Which Prohibits the Sending of Commercial Unsolicited Messages (SPAM), enacted on August 8, 2014 ('SPAM Law No. 310- 14',) also provides criminal sanctions for fraudulently obtaining personal data from public websites for commercial purposes (including imprisonment ranging from six months to five years, and fines from 1 to 200 times the minimum wage).

Although the National Institute for the Protection of Consumer Rights, "Pro Consumidor" cannot impose fines or administrative sanctions but conciliation and arbitration processes between users, consumers and suppliers can be initiated before them.

ELECTRONIC MARKETING

Sending commercial or promotional communications via electronic mail is regulated by SPAM Law 310-14. Law 310-14 requires the consent of the recipient in order to deliver commercial communications, unless an exception to said consent requirement is expressly provided by law.

Law 310-14 provides that:

- The word 'Publicity' (*Publicidad*) must be included in the subject field of the email
- Commercial communications must include an email address or other similar mechanism which allows the recipient to send a message indicating their desire to stop receiving such communications (opt-out)

ONLINE PRIVACY

The Dominican Republic has not enacted specific legislation governing online privacy or the use of ‘cookies’, although the provisions of the DPL concerning data protection would apply.

Additionally, the unauthorized use of ‘cookies’ could implicate computer misuse laws prohibiting unauthorized access to computers and information therein, particularly those contained in Law No. 53-07 on high-tech crimes and felonies.

KEY CONTACTS

Mary Fernandez
Founding Partner
Headrick
T +809 473 4500
mfernandez@headrick.com.do

Fernando J. Marranzini
Partner
Headrick
T +809 473 4500
fmarranzini@headrick.com.do

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ECUADOR

Last modified 26 January 2023

LAW

Constitution

The Constitution of Ecuador in its article 66, referring to the personal freedom rights of individuals in the Ecuadorian territory, the State recognizes and guarantees in section 19: "*The right to the protection of personal data, which includes the access and decision on information and data of this nature, as well as its corresponding protection. The collection, filing, processing, distribution or dissemination of such data or information shall require the authorization of the owner or the mandate of the law.*"

Article 92 gives the right to every person to be informed of and have access to information, documents, genetic data, personal data banks or files and reports on him/herself and his/her assets, contained in files and/or databases of public or private entities, in material and/or electronic support. The interested individual has the right to be informed of the use, purpose, origin and destination of his personal data and the time of permanence of the file of the same.

The responsible parties of the personal data banks or files may disseminate the information filed with the authorization of its owner, before which the owner of the personal data may request from the responsible party access to the file free of charge, as well as the updating, rectification, deletion or cancellation of his personal data.

In the case of sensitive data, the collection and storage must be authorized by law or by the owner. The adoption of the necessary security measures will be required. If the request is not complied with, the affected individual may appeal to the judge and may sue for the damages caused.

Personal Data Protection Organic Law

Since May 26, 2021, Ecuador adopted the Personal Data Protection Organic Law, whose main purpose is to guarantee the right to the protection of personal data, that includes the access and decision on information and personal data, as well as its corresponding protection. The law mainly refers to the conditions that must be verified for the legitimate treatment of personal data. It also refers to the ways through which the owner of the personal data may express his or her consent to the processing of his or her data.

Regulation to the Personal Data Protection Organic Law

On November 13, 2021, the President of Ecuador issued the Regulation to the Personal Data Protection Organic Law, whose main purpose is to develop aspects already provided for in the law. Among the most important aspects of the Regulation are the specifications for requests related to the exercise of data protection rights, the notification of security breaches, data processing agreements, the data protection officer, and international data transfers.

DEFINITIONS

Definition of Personal Data

The Ecuadorian data protection regime distinguishes between personal data and a sub-category of sensitive personal data, depending on the information and the harmful effects caused by its unlawful use.

Article 4 of the Organic Law on Personal Data Protection defines personal information as the information that identifies or makes identifiable a specific individual, directly or indirectly.

Definition of Sensitive Personal Data

Article 4 of the Organic Law on Personal Data Protection defines sensitive personal data as information related to: ethnicity, gender identity, cultural identity, religion, ideology, political affiliation, judicial background, immigration status, sexual orientation, health, biometric data, genetic data and those whose improper processing may give rise to discrimination, infringe or may infringe fundamental rights and freedoms.

In application of article 26 of the Organic Law for the Protection of Personal Data, the processing of sensitive personal data is prohibited unless one of the following circumstances applies:

- The owner has given his explicit consent to the processing of his personal data, clearly specifying its purposes.
- The processing is necessary for the fulfilment of obligations and the exercise of specific rights of the controller or the holder in the field of labor law and social security and protection.
- The processing is necessary to protect the vital interests of the data owner or another individual, in the event that the data owner is physically or legally incapable of giving his/her consent.
- The processing relates to personal data which the data owner has manifestly made public.
- The processing is carried out by order of a judicial authority.
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which must be proportionate to the aim pursued, respect in substance the right to data protection and provide for adequate and specific measures to protect the interests and fundamental rights of the owner.
- When the processing of health data is subject to the provisions contained in this Law.

Definition of Large-Scale Data Processing

Article 4 of the Regulation to the Organic Law on Personal Data Protection defines large-scale data processing activities as the following:

- The processing of patients’ data in the normal course of activity of a hospital or health institution.
- The processing of travel data of persons using public transportation systems.
- The processing of real-time geolocation data of customers by a data controller specialized in the provision of these services.
- The processing of customer data in the normal course of business of an insurance company, brokers, agent or financial institution.
- The processing of personal data for behavioral advertising by a search engine.
- The processing of data (content, traffic, location) by telephone or Internet service providers.

Definition of Joint Controllers

Article 37 of the Regulation to the Organic Law on Personal Data Protection specifies that when two or more controllers jointly determine the same purposes of and means for the processing of personal data, they shall be considered joint controllers, who shall define their respective tasks and responsibilities regarding data protection in a transparent manner by means of a contract, insofar as these are not already defined by the law.

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to the provisions of Articles 76 and 77 of the Organic Law for the Protection of Personal Data, the Authority for the Protection of Personal Data will be the Superintendence of Data Protection, which once constituted will act as the control and

surveillance body in charge of guaranteeing all citizens the protection of their personal data, and of carrying out all necessary actions to ensure that the principles, rights, guarantees and procedures provided for in the Law and its implementing regulations are respected.

REGISTRATION

Article 51 of the Organic Law for the Protection of Personal Data creates the National Registry for the Protection of Personal Data, a registry that will be under the responsibility and custody of the Superintendence of Data Protection as the competent national protection authority. The person responsible for the processing of personal data shall report and keep updated the information before the Personal Data Protection Authority, on the following:

- Identification of the database treatment.
- Name, legal domicile, and contact details of the responsible and in charge individual of the processing of personal data. Characteristics and purpose of the personal data treatment.
- Nature of the personal data treatment.
- Identification, name, legal domicile, and contact details of the recipients of the personal data, including processors and third parties.
- Description of the utilized method of interrelation of the recorded information.
- Description of the means used to implement the principles, rights and obligations contained in the present Law and specialized regulations for the data protection.
- Requirements and/or technical and physical, organizational, and legal administrative tools implemented to guarantee the security and protection of personal data.
- Data retention time.

Article 87 of the Regulation to the Organic Law for the Protection of Personal Data creates the Registry of Defaulting Controllers and Processors, under the responsibility and custody of the Superintendence of Data Protection, exclusively for purposes of statistics, prevention and training.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer (DPO) if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities, provided that it does not give rise to a conflict of interests.

DPOs must exercise their duties in a "*professional manner*" for the controller or processor, though it is possible to outsource the DPO role to a service provider.

The DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks.

The specific tasks of the DPO include:

- to inform and advise on compliance with the Personal Data Protection Organic Law;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the Superintendence of Data Protection.

COLLECTION & PROCESSING

Our Personal Data Protection Law defines data processing as any operation or set of operations performed on personal data, whether by automated, partially automated or non-automated technical procedures, such as: collection, compilation, obtaining, recording, organization, structuring, conservation, custody, adaptation, modification, elimination, indexing, extraction, consultation, processing, use, possession, exploitation, distribution, assignment, communication or transfer, or any other form of enabling access, matching, interconnection, limitation, suppression, destruction and, in general, any use of personal data.

The processing of personal data shall be legitimate and lawful if any of the following conditions are met:

1. By consent of the owner for the treatment of his personal data, for a specific purpose or purposes.
2. That it is carried out by the data controller in compliance with a legal obligation.
3. That it is carried out by the data controller, by court order, in compliance with the principles of the present Law.
4. That the treatment of personal data is based on the fulfilment of a mission carried out in the public interest or in the exercise of public powers conferred on the controller, derived from a competence attributed by a regulation with the rank of law, subject to compliance with the international human rights standards applicable to the matter, to compliance with the principles of this Law and to the criteria of legality, proportionality, and necessity.
5. For the execution of pre-contractual measures at the request of the owner or for the fulfilment of contractual obligations pursued by the person responsible for the processing of personal data, person in charge of the processing of personal data or by a legally authorized third party.
6. To protect vital interests of the data subject or another natural person, such as his or her life, health, or integrity.
7. For the processing of personal data contained in publicly accessible databases; or
8. To satisfy a legitimate interest of the data controller or of a third party, provided that the interest or fundamental rights of the data subjects do not prevail under the provisions of this regulation.

Personal data may be processed and communicated when there is an explicit consent of the owner to do so. The consent will be valid when the expression of will is:

1. Free, that is, when it is absent of any consent flaws.
2. Specific, in terms of the concrete determination of the means and purposes of the data treatment.
3. Informed, so that it complies with the transparency principle.
4. Unambiguous, so that there is no doubt as to the scope of the authorization granted by the owner.

The consent of the data owner must reflect, in an unequivocal manner, his or her acceptance in relation to the processing of personal data. Silence or inaction, by itself, does not imply the consent of the data owner.

Consent may be revoked at any time without the need for a justification, for which purpose the data controller shall establish mechanisms that guarantee speed, efficiency, effectiveness, and gratuity, as well as a simple procedure, similar to the procedure by which the consent was obtained.

The processing carried out prior to the revocation of consent is lawful since it does not have retroactive effects.

When the data treatment is intended to be based on the consent of the data owner for a plurality of purposes, it will be necessary to state that such consent is obtained for all of them.

Unless proven otherwise, it shall be legitimate and lawful to process data intended to provide information on the financial or credit solvency, including information relating to the fulfilment or non-fulfilment of obligations of a commercial or credit nature that enable an assessment on the general conclusion of business, the commercial conduct or the payment capacity of the owner of the information, where such information is obtained from publicly available sources or from information provided by the creditor. Such data may be used only for the purpose of analysis and will not be communicated or disseminated, nor may they be used for any secondary purpose.

The protection of personal credit data shall be subject to the provisions of this Law, the specialized legislation on the subject and other regulations issued by the Personal Data Protection Authority.

Notwithstanding the foregoing, in no case may credit data relating to obligations of an economic, financial, banking or commercial nature be communicated after five years have elapsed since the obligation to which they refer has become due.

Pursuant to the provisions of article 29 of the Organic Law on Personal Data Protection, the holders of Credit Data have the following rights:

1. To have personal access to the information of which they are owners.
2. That the credit report allows them to know the condition of their credit history clearly and precisely; and,
3. That the sources of information update, rectify or eliminate information that is unlawful, false, inaccurate, erroneous, incomplete, or outdated.

Regarding the right of access by the Credit Data Owner, this shall be free of charge, as many times as required, with respect to the information registered about him/herself before the credit reference service providers and through the following mechanisms:

1. Direct observation through displays that the credit reference service providers will make available to such owners; and
2. Delivery of printed copies of the reports for the Credit Data Subject to verify the truthfulness and accuracy of their content, without being used for credit or commercial purposes.

Regarding the rights of updating, rectification or deletion, the Data Owner may demand these rights from the information sources by means of a written request. The information sources, within fifteen days from the date the request is submitted, shall resolve it by admitting or rejecting it with reasons. The Credit Data Owner has the right to request the credit reference service providers to indicate in the credit reports they issue, while the review process continues, that the information subject to the request is being reviewed at the owner's request.

TRANSFER

Personal data may be transferred or communicated to third parties when it is carried out for the fulfillment of purposes directly related to the legitimate functions of the controller and the recipient, when the transfer is configured within one of the grounds of legitimacy and also has the consent of the owner.

It shall be understood that the consent is informed when for the transfer or communication of personal data the data controller has provided sufficient information to the data subject to enable him/her to know the purpose for which his/her data will be used and the type of activity of the third party to whom it is intended to transfer or communicate such data.

It will not be considered a transfer or communication in the event that the processor or a third-party accesses personal data for the provision of a service to the controller of personal data. The third party who has legitimately accessed personal data in these considerations shall be considered the processor.

The treatment of personal data carried out by the processor or by a third party must be regulated by a contract, in which it is clearly and precisely established that the personal data processor or the third party will only process the information in accordance with the instructions of the owner and will not use it for purposes other than those indicated in the contract, nor transfer or communicate it even for storage to other persons.

The contract between controller and processor must contain provisions specifying at least the following:

- Object
- Duration
- Nature
- Purposes of the processing activities
- Categories of personal data
- Data owners
- Obligations and responsibilities of the processor

Once the contractual performance has been fulfilled, the personal data shall be destroyed or returned to the data controller under the supervision of the Personal Data Protection Authority.

The processor or third party shall be liable for any infringements arising from non-compliance with the conditions of personal data processing set forth in this Law.

The processor may engage a third party to supplement the provision of a service to the controller of personal data, provided that this is expressly stated in the processing agreement. Otherwise, it shall require the written authorization of the controller for the subcontracting.

SECURITY

Data controllers or the individual in charge of the treatment of personal data must abide by the principle of personal data security, for which it must consider the categories and volume of personal data, the state of the art, best comprehensive security practices. and the costs of application according to the nature, scope, context, and purposes of the treatment, as well as identifying the probability of risks.

Data controllers or the individual in charge of the treatment, must implement a process of verification, evaluation and continuous and permanent assessment of the efficiency, effectiveness, and effectiveness of the measures of a technical, organizational and any other nature, implemented to guarantee and improve the security of the processing of personal data.

The individual in charge of the treatment of personal data must demonstrate that the measures adopted and implemented adequately mitigate the risks identified.

Among other measures, the following may be included:

- Anonymization, pseudonymization or encryption measures of personal data.
- Measures aimed at maintaining the confidentiality, integrity and permanent availability of the systems and services for the processing of personal data and access to personal data, quickly in case of incidents.
- Measures aimed at improving technical, physical, administrative, and legal residence.
- Those responsible and in charge of the treatment of personal data, may avail themselves of international standards for adequate risk management focused on the protection of rights and freedoms, as well as for the implementation and management of information security systems or codes of conduct. recognized and authorized by the Personal Data Protection Authority.

BREACH NOTIFICATION

Mandatory breach notification

Data controllers or the individual in charge of the treatment of personal data must notify the breach of personal security data to the Personal Data Protection Authority and the Telecommunication Control Agency, as soon as possible, and at the latest within a term of five (5) days after the occurred breach incident, unless it is unlikely that said breach of security constitutes a risk to the rights and freedoms of its individual owners. If the notification to the Data Protection Authority does not take place within five (5) days, it must be accompanied by an indication of the reasons for the delay.

According to the Regulation to the Personal Data Protection Organic Law, the following circumstances are deemed a risk to the rights and freedoms of persons:

1. When the data have been destroyed, no longer exist or are not available in a form that is useful to the data controller.
2. When the personal data have been altered, corrupted or are no longer complete.
3. When the controller has lost control or access to the data, or the data is no longer in its possession.
4. When the processing has not been authorized or is unlawful, which includes the disclosure of personal data or access by recipients or third parties who are not authorized to receive or have access to the data, or any other form of processing that is executed contrary to the provisions of the Law.

The data breach notification must provide for the following aspects:

- The nature and type of breach.
- Data owners or interested parties affected.

- Breached systems.
- Presumed cause of the breach.
- Volume and types of compromised or exposed data.
- Response and mitigation measures.
- Risk assessment for the rights and freedoms of the data owners.

Data controllers or the individual in charge of the treatment of personal data must notify the person in charge of any violation of the security of personal data as soon as possible, and at the latest within a term of two (2) days from the date on which he becomes aware of it.

The person responsible for the treatment must notify the owner of the breach of personal data security without delay when it entails a risk to their fundamental rights and individual freedoms, within a term of three (3) days from the date on which they became aware of the risk.

ENFORCEMENT

In case of non-compliance with the provisions set forth in the Law, its regulations, guidelines and directives and regulations issued by the Personal Data Protection Authority, the Personal Data Protection Authority shall issue corrective measures with the purpose of preventing the infringement from continuing and the conduct from occurring again, without prejudice to the application of the corresponding administrative sanctions.

Corrective measures may consist of, among others:

1. The cease of the treatment, under certain conditions or deadlines.
2. The disposal of the data; and,
3. The imposition of technical, legal, organizational or administrative measures to ensure proper handling of personal data.

The Personal Data Protection Authority, within the framework of this Law, will dictate, for each case; the corrective measures, which are classified into minor infringements and serious infringements.

Penalties for minor infringements will impose an administrative sanction of a fine between 0.1% and 0.7% calculated on the turnover corresponding to the financial year immediately prior to the imposition of the fine.

Penalties for serious infringements will impose an administrative sanction of a fine between 0.7% and 1% calculated on the turnover corresponding to the financial year immediately prior to the imposition of the fine.

In addition to the previously mentioned fines, the Personal Data Protection Authority may apply provisional measures of protection or precautionary measures such as:

1. Seizure.
2. Withholding.
3. Sale Prohibitions.
4. Shutdown of establishments.
5. Activity suspension.
6. Decommissioning of products, documents, or other goods.
7. Eviction of individuals.

ELECTRONIC MARKETING

There is no specific regulation regarding data treatment on electronic marketing, to the extent that it may involve processing of personal data, is subject to the general rules applicable to such data, such as valid data subject consent, adequate privacy notices as to use and disclosure of personal data and data subject rights.

ONLINE PRIVACY

There is no specific regulation regarding processing of personal data online, therefore, this kind of processing shall be ruled by the Personal Data Protection Organic Law.

Personal data must not be available online unless there are adequate security measures to ensure that access by any unauthorized user is restricted.

The use of cookies in web pages is forbidden unless the data subject has given an authorization for usage which may be obtained by a pop-up informing the user about the privacy policy and the way to disable cookies. All the other tracking systems need proper authorization from the data subject.

Unauthorized collection of personal data will be subject to the general rules applicable to such data.

KEY CONTACTS

Bustamante Fabara
bustamantefabara.com/

José Rafael Bustamante Crespo
Partner
Bustamante Fabara
jrbc@bustamantefabara.com

Gino Ivich Jijón
Associate
Bustamante Fabara
T +593998546947
givich@bustamantefabara.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

EGYPT

Last modified 19 January 2024

LAW

Personal Data Protection Law No.151 of 2020 (the "Law").

DEFINITIONS

Definition of Personal Data

Pursuant to Article (1) of the Law, personal data shall mean any data relating to an identified natural person, or one who can be identified directly or indirectly by way of linking such personal data and other data such as name, voice, picture, identification number, online identifier, or any data which determines the psychological, medical, economic, cultural or social identity of a natural person.

Definition of Sensitive Personal Data

Pursuant to Article (1) of the Law, sensitive data shall mean data which discloses psychological, mental or physical health, or genetic, biometric or financial data, religious beliefs, political views, or criminal records. In all cases, data relating to children is considered to be sensitive personal data.

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to Article (19) of the Law, the Personal Data Protection Centre (the "Centre") is a public economic authority that has a legal personality and is under the authority of the Minister of Communications and Information Technology. Such authority aims to protect personal data and regulate the activities of processing and granting access to such personal data. The Centre shall practice all the competences stipulated by the Law for achieving its objectives. Particularly, the Centre has the following competences:

- Setting and developing the policies, strategy plans and the programs necessary for protecting personal data and the execution thereof;
- Unifying the policies and plans for protecting and processing personal data within the Arab Republic of Egypt;
- Setting and applying the decisions, regulations, measures, procedures and criteria related to the protection of personal data;
- Setting a guidance framework for the codes of conduct related to the protection of personal data and approving the codes of conduct of different entities;
- Organizing and cooperating with all the entities, governmental and non-governmental bodies in guaranteeing personal data protection measures and connecting with all the related initiatives;
- Supporting the development of the competence of the personnel working in all governmental and non-governmental entities who are competent with the protection of personal data;

- Issuing licenses, permits, certifications and various measures related to the protection of personal data and the enforcement of the provisions of the Law;
- Accrediting the entities or individuals and granting them the required permits to provide consultation in relation to personal data protection measures;
- Receiving complaints and communications related to the provisions of the Law and issuing the necessary decisions in this regard;
- Advising on draft laws and international agreements which are related to, regulating, or affecting the personal data directly or indirectly;
- Controlling and inspecting the addresses of the provisions of the Law, and take the necessary legal procedures;
- Verifying the conditions of cross-border personal data transfer and issuing the decisions regulating the same;
- Organizing conferences, workshops, training and educational courses and issuing publications to raise awareness and to educate individuals and entities about their rights in relation to dealing with personal data;
- Providing all types of expertise and consultations related to the protection of personal data, in particular to the investigation and judicial authorities;
- Entering into agreements and memoranda of understanding, coordinating cooperating, and knowledge exchange agreements, with international entities, which are relevant to the Centre’s work;
- Issuing circulars which update the personal data protection measures, in accordance with the activities of different sectors and with the Centre’s recommendations; and
- Preparing and issuing an annual report on the status of protection of personal data in the Arab Republic of Egypt.

REGISTRATION

Pursuant to the Law, the controller or the processor must obtain a license or a permit from the Centre for practicing the activity of collecting, storing, transferring, or processing electronic personal data, sensitive data or to undertake any electronic marketing activities.

Applications for licenses, permits, and certifications shall be submitted on the forms produced by the Centre together with all of the supporting documents and information requested to be submitted, along with proof of the applicant's financial ability and its ability to implement the stipulated requirements and technical standards. Decisions on the applications shall be made within a period not exceeding ninety (90) days from the date of completing all documentation and information. The lapse of the above-mentioned period without any decision shall be deemed rejection of the application.

Pursuant to Article (26) of the Law, the licensing fee shall not exceed EGP 2,000,000 (two million Egyptian pounds), while permits or certifications shall not exceed EGP 500,000 (five hundred thousand Egyptian pounds).

DATA PROTECTION OFFICERS

Pursuant to Article (8) of the Law, the legal representative of the juristic person of any of the controller or the processor shall appoint a competent employee as a Data Protection Officer (the “DPO”) within its entity to be responsible for personal data protection. Such DPO must be registered on the DPO register at the Centre. The DPO shall be responsible for enforcing the provisions of the Law and the decisions of the Centre, as well as monitoring and supervising the procedures applicable within the entity and receiving requests related to personal data. The DPO shall, in particular undertake the following:

- Perform a regular evaluation and inspection of the personal data protection systems and avoid infringement thereto as well as documenting the results of such evaluation and issuing the necessary recommendations for its protection.
- Act as a direct contact point with the Centre and implement its decisions, with respect to the application of the provisions of the Law.
- Enable the data subject to practice its rights stipulated under the Law.
- Notify the Centre of the occurrence of any breach of personal data within his entity.
- Reply to the requests submitted by the data subject or any relevant person and reply to the complaints filed by them to the Centre.
- Follow-up the registration and update the personal data records held by the controller, or the processing activity records held by the processor, to guarantee the accuracy of the data and information recorded therein.

- Eliminate any transgressions related to personal data within its entity and undertaking the corrective actions related thereto.
- Organise the necessary training programs for the employees of the relevant legal entity, which are required to have sufficient qualifications that comply with the requirements stipulated by the Law.

COLLECTION & PROCESSING

Data Protection Principles

Controllers and processors must comply with a set of rules governing the processing of personal data. Pursuant to the Law, the following conditions must be fulfilled in order to collect, process and retain personal data:

- Personal data shall be collected for legitimate and specific purposes that shall be disclosed to the data subject.
- Personal data shall be correct, valid, and secured.
- Personal data shall be processed in a legitimate manner and in compliance with the purposes for which it is being collected.
- Personal data shall not be retained for a period longer than that is necessary for the fulfilment of the purpose thereof.

Processing Conditions

Pursuant to Article (6) of the Law, the electronic processing of personal data shall be considered legitimate and legal in cases where it satisfies one of the following conditions:

- It is carried out with the data subject’s consent for the achievement of certain purpose(s);
- It is necessary and intrinsic for the performance of a contractual obligation or legal action, the execution of an agreement for the benefit of the data subject, or the undertaking of any procedure with respect to claiming or defending the data subject's legal rights;
- It is necessary for performing a legal obligation or an order issued by the competent investigation authorities or it is based upon a judicial ruling; or
- It is necessary for enabling the controller to perform its obligations or any relevant person to practice its legitimate rights unless this contradicts the data subject’s fundamental rights and freedoms.

Rights of Data Subjects

Pursuant to Article (2) of the Law, personal data may not be collected, processed, disclosed, or revealed by any means except with the explicit consent of the data subject or where otherwise permitted by law.

Further, the data subjects have a range of rights to control the processing of their personal data, which are as follows:

- To know, review and access / obtain his / her own personal data, which is in possession of any holder, controller or processor;
- To withdraw the prior consent concerning the retention or processing of his/her personal data;
- To correct, edit, erase, add or update his / her personal data;
- To limit the processing to a specified purpose;
- To be notified with any infringement to his / her personal data; and
- To object to the processing of personal data or its results whenever this contradicts the data subject’s fundamental rights and freedoms.

Obligations of the Controller and the Processor:

Pursuant to chapter (3) of the Law, the controller and the processor must comply with certain conditions while collecting and processing personal data, *inter alia*:

- Ensure the validity, conformity and sufficiency of the personal data with the purpose of its collection;

- Not exceed the purpose and period of processing, and notify the controller, the data subject or each relevant person, as the case may be, with the period necessary for processing;
- Set the method, manner, and standards for processing pursuant to the designated purpose;
- Ensure the applicability of the specified purpose for the collection of the personal data for processing objectives;
- Refrain from undertaking any action which would result in disclosing personal data except in the cases permitted by law;
- Adopt all technical and regulatory procedures and apply the necessary standard criteria for protecting personal data and ensuring its confidentiality, and prevent any hack, damage, alteration or manipulation through any illegitimate procedure;
- Correct any error in the personal data immediately upon being notified or becoming aware of such error; and
- Avoid any direct or indirect harm to the data subject.

TRANSFER

Pursuant to Article (14) of the Law, it is prohibited to transfer any personal data that was collected or prepared for processing to a foreign country unless such country grants a level of protection of personal data, that does not fall below what is stipulated in the Law and subject to obtaining a relevant license or permit from the Centre. However, exceptions are made under Article (15) of the Law, if the direct consent of the data subject or his representative is obtained for transferring, sharing, circulating or processing personal data to a country that does not offer the same level of protection in the following cases:

- To protect the data subject’s life and provide them with medical care, treatment, or the administration of medical services.
- To perform obligations in order to prove the existence of a legal right or to exercise or defend such right before the judiciary.
- To conclude or perform an agreement entered into by the person responsible for processing the personal data and third party, which shall be in favor of the concerned data subject.
- To perform a procedure required under an international judicial cooperation.
- There is legal necessity or obligation to protect the public interest.
- To transfer money to another country pursuant to the laws in force of that country.
- If the transfer or circulation is pursuant to a bilateral or multilateral agreement, to which the Arab Republic of Egypt is a party.

In addition, the controller or the processor may, as the case may be, grant access to personal data to another controller or processor outside the Arab Republic of Egypt by virtue of a license from the Centre provided that the following conditions have been met:

- There is conformity between the nature of work of either of the controllers or processors, or unity between the purposes for which they obtain the personal data.
- Either the controllers or processors, or the data subject, have a legitimate interest in the personal data.

The level of legal and technical protection of the personal data offered by the controller or the processor abroad shall not fall below the level of protection provided in the Arab Republic of Egypt.

SECURITY

The Law defines data security as the technological and organizational procedures and operations for the purpose of protecting the privacy, secrecy, safety, unity, and completeness of personal data.

The Law does not state any specific technical standards or measures. However, the Law states that the controller must adopt all technical and regulatory procedures and apply the necessary standard criteria for protecting personal data and to ensure its confidentiality, and prevent any hack, damage, alteration or manipulation through any illegitimate procedure.

Furthermore, Article (25) of the Egyptian Anti-Cybercrimes Law imposes penalties of imprisonment for a period not less than six (6) months and/or a fine not less than EGP 50,000 (fifty thousand Egyptian pounds) and not exceeding EGP 100,000 (one hundred thousand Egyptian pounds). This penalty is imposed regardless of whether the published information is correct or incorrect, on

whoever violates the right to privacy, grants any personal data to a system or a website or sends densified e-mails without the data subject’s consent in order to promote goods or services or to publish information, news, pictures or the like, through the information network or by any means of information technology.

BREACH NOTIFICATION

Pursuant to Article (7) of the Law, each of the controller and the processor, as the case may be, shall notify the Centre with any personal data infringement, within seventy-two (72) hours of such infringement. In the event that such infringement relates to national security protection concerns, the notification shall be immediate. In all events, the Centre shall immediately notify the National Security Authorities with the infringement and provide them, within seventy-two (72) hours from being aware of the infringement, with the following:

- description of the nature of the infringement, the form and the reasons thereof as well as the approximate number of personal data and their records;
- the information of the DPO;
- the potential consequences of the infringement;
- description of the procedures which have been followed and the proposed procedures to be adopted in order to minimize the negative impacts of the infringement;
- evidence of documenting any personal data infringement and the corrective actions which have been taken to solve it; and
- any documents, information or data requested by the Centre.

In all events, the Controller and Processor, as the case may be, shall notify the data subject within three (3) days from the date of notifying the Centre, with the infringement and the adopted procedures related thereto.

The Law defines the National Security Authorities as the Presidency, Ministry of Defence, Ministry of Interior, the General Intelligence Directorate, and the Administrative Control Authority.

ENFORCEMENT

Right to Raise Complaints

Pursuant to Article (33) of the Law, the data subject and any relevant person, has the right to submit a complaint in relation to:

- Infringement or breach of the right of protection of personal data.
- Failure to enable the data subject to exercise his/her rights.
- The decisions issued by the DPO of the processor or controller in relation to the requests submitted to him/her.

Judicial Control Powers

The Centre’s employees, who are appointed by a decision of the Minister of Justice upon the proposal of the Minister of Telecommunications and Information Technology who is the competent minister in this regard, shall have judicial control powers in relation to violations of the Law.

Penalties

Failure to comply with the provisions of the Law, shall be penalized with imprisonment and/or fines that can reach up to EGP 5,000,000 (five million Egyptian pounds).

ELECTRONIC MARKETING

Pursuant to Article (17) of the Law, any electronic communication for the purpose of direct marketing to the data subject shall be prohibited unless the following conditions are met:

- consent is obtained from the data subject;
- the communication includes the identity of its creator and sender;
- the sender has a valid and complete address to be contacted at;

- the purpose is clearly indicated as being for direct marketing; and
- clear and uncomplicated mechanisms are set to allow the data subject to refuse the electronic communication or to withdraw his/her consent to receive such communication.

Further, Article (18) of the Law, provides that the sender of any electronic communication for direct marketing purpose shall undertake to do the following:

- specify a defined marketing purpose;
- not to disclose the contact details of the data subject; and
- maintain electronic records evidencing the consent of the data subject to receive electronic marketing communication and any amendments thereof, or their non-objection to its continuity for a duration of three (3) years from the date of sending the last communication.

ONLINE PRIVACY

The Law does not provide any specific rules for governing cookies and location data. However, pursuant to Article (2) of the Egyptian Anti-Cybercrimes Law No. 175 of 2018, the service providers are under a duty to maintain the privacy of the data stored and not to disclose it to anyone without a reasoned order from a relevant judicial authority. Such duty includes the personal data for any of the users of the service provided by such service provider. A service provider who violates this duty shall be penalized with imprisonment for a period not less than one (1) year and/or a fine not less than EGP 5,000 (five thousand Egyptian pounds) and not exceeding EGP 20,000 (twenty thousand Egyptian pounds).

Furthermore, Article (25) of the Anti-Cybercrimes Law imposes penalties of imprisonment for a period not less than six (6) months and/or a fine not less than EGP 50,000 (fifty thousand Egyptian pounds) and not exceeding EGP 100,000 (one hundred thousand Egyptian pounds). This penalty is imposed regardless of whether the published information is correct or incorrect, on whoever violates the right to privacy, grants any personal data to a system or a website or sends densified e-mails without the data subject’s consent in order to promote goods or services or to publish information, news, pictures or the like, through the information network or by any means of information technology.

KEY CONTACTS

Matouk Bassiouny & Hennawy
matoukbassiouny.com/the-firm/

Nevine Aboualam
Partner
Matouk Bassiouny & Hennawy
T + (202) 2796 2042 (ext.111)
nevine.aboualam@matoukbassiouny.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

EL SALVADOR

Last modified 28 January 2024

LAW

N/A.

El Salvador’s Congress approved a Personal Data Protection Act on Apr. 22, 2021. As part of the process of creation of a Law in El Salvador, all Acts approved by Congress are later referred to the President of the Republic for his review/veto/approval. In this case, the Act was vetoed and sent back to Congress for review but no further action has been taken in order to review the causes for the veto and/or make any amendments for its further approval.

Hence, data protection regulation in El Salvador remains disseminated in many other Acts that briefly regulate the confidentiality of a person’s information but no specific regulation is in place.

DEFINITIONS

Definition of Personal Data

> “Information concerning a natural/moral person who is identified or identifiable.”

Definition as contained Personal Data Protection Act on Apr. 22, 2021

Definition of Sensitive Personal Data

> “Personal data that affects the most intimate sphere of its owner and whose misuse may give rise to discrimination, seriously affect the right to honour, personal and family privacy and self-image. They are generally those that reveal aspects such as creed, religion, ethnic origin, political affiliation or ideologies, union membership, sexual preferences, physical and mental health, biometric information, genetics, moral and family situation, and other intimate information of a similar nature.”

Definition as contained Personal Data Protection Act on Apr. 22, 2021

NATIONAL DATA PROTECTION AUTHORITY

The Personal Data Protection Act on Apr. 22, 2021 created the National Authority for the Protection of Personal Data; however, said institution is not in force given that the Act was not finally approved.

Some protection of data is handled by the Institution of Access to Public Information but in regards specifically to data of persons who have had a direct relationship with the Government, such as current or former public employees, contractors, etc.

REGISTRATION

Registration is not regulated.

DATA PROTECTION OFFICERS

To this date, only Public Offices/Institutions are required to appoint a Public Information Access Officer, but no Data Protection Officer regulation is in place.

COLLECTION & PROCESSING

Collecting and Processing is not specifically regulated. However, the E-Commerce Act establishes, in general terms, that all information provided by the user of an online store/marketplace must be safely guarded. Similar requirements are established by the E-Signature Act, in regards to the information of the owners of an E-Signature.

TRANSFER

Transfer is not specifically regulated. However, disperse regulation generally establishes that the owner of personal information must authorise in written the transfer of their data.

SECURITY

Security is not specifically regulated. However, the E-Commerce Act establishes, in general terms, that all information provided by the user of an online store/marketplace must be safely guarded. Similar requirements are established by the E-Signature Act, in regards to the information of the owners of an E-Signature.

BREACH NOTIFICATION

Breach notification is not regulated.

ENFORCEMENT

No specific Enforcement Authority has been created. However to the extent of its capabilities and within the legal framework of our criminal jurisdiction, the General Attorney’s Office can prosecute any crime related with the use of personal data as regulated in the laws of the matter.

ELECTRONIC MARKETING

Electronic Marketing is not specifically regulated; however, false/misleading advertisement is punishable as stated in El Salvador’s Consumer Protection Act.

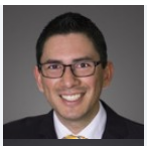
ONLINE PRIVACY

No specific regulation is in place regarding online privacy in El Salvador.

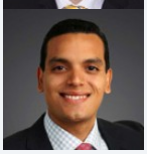
KEY CONTACTS

Central Law
central-law.com

Fernando Argumedo
Associate



Central Law
T +503 2241 3600
fargumedo@central-law.com



Francisco Murillo
Associate
Central Law
T +503 2241 3600
fmurillo@central-law.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

EQUATORIAL GUINEA

Last modified 10 January 2022

LAW

The applicable law is the Personal Data Protection Law Num. 1/2016 dated 22 July.

DEFINITIONS

Definition of Personal Data

The Personal Data Protection Law under art.4 defines personal data as "*any information, testimony or review concerning a person specifically identified or identifiable*".

Definition of Sensitive Personal Data

The law does not provide a definition of sensitive personal data. However, art.41(d) consider as a mayor infringement the treatment or given out of personal data in relating to conscience liberty, affiliation or political ideology, health, sex life, race, tribe, religion or any other discrimination form without the express authorization of the owner.

NATIONAL DATA PROTECTION AUTHORITY

The Governing Data Protection Body.

REGISTRATION

The General Data Protection Registry (art. 33) is the organ responsible for registration under its Technical Secretariat which takes charge of the registration of public and private personal data files and of carrying out all actions entailing the modification, creation or suppression of personal data through authorised books.

DATA PROTECTION OFFICERS

The Governing Data Protection Body through its Technical Secretariat is responsible for ensuring the administration of personal data files, regardless of their ownership, is done in due compliance with the provisions of the law.

COLLECTION & PROCESSING

Arts. 6 and 9 of the applicable law determines that only personal data that are adequate, accurate, truthful, complete and not excessive in relation to the scope and purpose of their collection may be used, prohibiting the collection of such data by fraudulent and unlawful means.

In this regard, an interested parties to whom personal data are requested must be previously expressly informed in a concise and unequivocal manner and must be informed about the purpose and consequences of the collection, the destination and the

recipients of the information, about the mandatory or optional nature of their response to the questions asked, about the effects of the refusal to provide them, as well as the identity and address of the person responsible for the processing or its representative.

The processing of data by third parties according the law must be subject to a contractual agreement under which a third parties must agree in writing to process the data solely and in accordance with the instructions authorised by the owner, that is, the data must not be used or applied for a different purpose or communicated to third parties (art.8).

TRANSFER

Art. 21 is to the effect that:

- Personal data obtained by the General administration of the state cannot be communicated or given out unless it is for historic or, statistics of scientific purposes. However, personal data could be communicated between the public administration and other public organs or institutions.
- Private holders of personal data cannot communicate or give out personal data found in their possession unless by a court order instructed by a competent court.
- For the performance of any of the above, the holders of the data have to be notified of the purpose for which their data is to be communicated or given out. Notwithstanding, consent will not be needed from the owner of the data unless the data was made available to the public, and it is likely to be communicated to other public or private files.

SECURITY

Art. 11 determines that, the data controller or data processor must adopt the necessary technical and organisational measures to ensure the security of the personal data processed, ensuring their preservation and avoiding their alteration, loss, unauthorised processing or access. In this sense, personal data must not be recorded in files, systems or processing centres that do not meet the security conditions for the integrity, confidentiality and guarantee of the same.

BREACH NOTIFICATION

The breach of notification constitutes a minor infringement when the data was obtained from the person concerned (art. 39 C) and a major infringement when the data was not obtained from the person concerned (art. 40 C).

Mandatory breach notification

The law does provide for a mandatory breach duty. Notwithstanding, it provides that in the case of a severe or major breach likely to affect a fundamental right or personal data the sanctioning organ may require the person responsible to restrain the use, communication, give out, or the illegal transfer.

ENFORCEMENT

The enforcement process applied to determine and impose the sanctions is adjusted to the principles, rules and norms of administrative procedure at the request of an audience by the interested party. During the audience, other enforcement measures can be adopted by the sanctioning organ to ensure compliance of the final resolution and to secure the application of the sanctions. However, these measures have a provisional character (art.45).

Where the infringement is committed in a public file, the sanctioning organ has to pass a resolution ordering the dismissal or correction of the infringement, as well as propose the application of disciplinary proceedings against the offenders (art.45).

The resolution of the sanctioning organ is elevated to a higher authority, which must then verify and determine the applicable sanctions against the infringement.

ELECTRONIC MARKETING

Not regulated by the personal data protection law. However, art. 22 of the Internet Communication Law Num. 1/2017 dates January is to the effect that commercial electronic communications such as adverts and promotions must conform with the data protection laws in relation to the abstention, creation and maintenance of files. More also, data used for such purposes must be clear and identifiable.

ONLINE PRIVACY

Not regulated by the law.

KEY CONTACTS

Centurion Law Group
centurionlg.com/

Maria Cheswa Alogo Django
Junior Associate
Centurion Law Group
T 00240 222 378 493
maria.django@centurionlg.com

Pablo Mitogo
Associate
Centurion Law Group
T 00240 222 762 410
pablo.mitogo@centurionlawfirm.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ESTONIA

Last modified 19 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

In Estonia, all derogations / additional requirements to the GDPR are provided in the new Personal Data Protection Act (PDPA) and the Personal Data Protection Implementation Act (Implementation Act).

The new PDPA was adopted by the Estonian parliament on December 12, 2018 and entered into force on January 15, 2019. The Implementation Act was adopted on February 20, 2019 and entered into force on March 15, 2019.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor " *processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The PDPA and the Implementation Act use the same definitions as the GDPR and do not foresee any new terms or terms defined differently from the GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The PDPA specifies that in the meaning of Article 51(1) of the GDPR the independent supervisory authority of Estonia shall be the Estonian Data Protection Inspectorate (DPI). The PDPA further specifies the requirements for and appointing of the head of the DPI.

In addition to the tasks provided in Article 57 of the GDPR, the PDPA specifies that the DPI is competent to:

- raise awareness and understanding of the public, the controllers and processors about the risks of processing personal data, the standards and safeguards applicable to processing, and the rights related to the processing of personal data; The DPI may provide indicative guidance for this task;
- provide information to the data subject, upon request, about the exercise of his rights under this PDPA and, if necessary, cooperate with other supervisory authorities of the European Union Member States for this purpose;
- initiate, where necessary, misdemeanor proceedings and impose sanctions in the event where it is not possible to achieve compliance with the requirements provided by law or GDPR with the application of other administrative measures;

- cooperate with international data protection supervisory organizations and other data protection supervisory authorities and other competent authorities and persons of foreign states;
- monitor relevant trends insofar as they affect the protection of personal data, in particular the development of information and communication technology;
- participate in the European Data Protection Board;
- apply administrative coercion to the extent and pursuant to the procedure prescribed by law;
- submit opinions to the Estonian parliament, the Government of the Republic, the Chancellor of Justice and other institutions and the public on its own initiative or upon request on issues related to the protection of personal data;
- perform other duties arising from law.

In addition to the rights and powers under the GDPR the PDPA specifies that the DPI has the right to:

- warn the controller and the processor that the data processing activities are likely to violate the PDPA;
- demand the rectification of personal data;
- demand the deletion of personal data;
- demand restriction of processing of personal data;
- demand the termination of the processing of personal data, including destruction or archiving;
- implement organizational, physical and informational security measures for the protection of personal data without delay, if necessary, in accordance with the procedure provided for by the Substitutive Enforcement and Penalty Payment Act, if necessary, in order to prevent damage to the rights and freedoms of a person, unless personal data are processed by a public authority;
- impose a temporary or permanent restriction on the processing of personal data, including a prohibition on the processing of personal data;
- initiate state supervisory proceedings on the basis of a complaint or on its own initiative.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Given that the GDPR does not provide for the registration of processing personal data, registries and systems will no longer exist. The PDPA specifies that pre-recorded data will remain as archived information about past activities for the term of up to five years after entry into force of the PDPA and upon expiry of the prior term (i.e. on 15 January 2024), pre-recorded data shall be erased.[1]

1: See Subsection 74(1) of the PDPA accompanied with Section 76 of the PDPA. PDPA is available in English here.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

In relation to DPOs, the PDPA and the Implementation Act do not foresee any derogations / additional requirements to the GDPR.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record- keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose;
- the context in which the data have been collected;
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible);
- the possible consequences of the new processing for the data subjects;
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to

requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorised by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

- Processing after data subject’s death. According to the PDPA the consent of the data subject is valid during the data subjects life and 10 years after the data subject’s death, unless otherwise provided by the data subject. If the data subject has died underaged, the data subject’s consent shall be valid for 20 years after his / her death. After the data subject’s death, the processing of his/her personal data is permissible upon the consent of one of the heirs of the data subject, unless:
    - 10 years have passed from the death of the data subject;
    - More than 20 years have passed from the death of an underaged data subject
    - Another legal basis for processing exists.

The aforementioned consent is not required when the processing includes only the data subject’s name, gender, time of birth and death, the fact of death, and the time and place of burial.

- Processing of personal data related to the breach of a contractual obligation. It is permitted to transfer personal data related to a breach of a contractual obligation to a third party, and the third party is permitted to process this personal data, with the purpose of assessing the creditworthiness of the data subject, or with another similar purpose, and only on condition that the controller or processor has checked the correctness of data, the legal basis for transfer and has registered the data transfer. Gathering data for the aforementioned purposes and transferring it to a third person is not permissible, if the data includes special categories of personal data, the data refers to the fact of being a victim of or committing an offence (before the public hearing, judgement or termination of proceedings), it would have a material adverse effect on the data subjects rights, or less than 30 days or more than 5 years has passed from the end of the breach of the obligation.

- Processing for journalistic purpose – GDPR article 85. It is permissible to process personal data without the data subject’s consent for journalistic purposes (primarily make information public in media) if public interest exists and such processing is done according to the principles of journalistic ethics. Such publicizing must not cause excessive damage to the rights of a data subject.

- Processing for the purposes of academic, artistic or literary expression – GDPR article 85. It is permissible to process personal data without the data subject’s consent for the purposes of academic, artistic or literary expression (primarily publication) if it does not cause excessive damage to the rights of the data subject.

- Processing of personal data in a public space. Unless the law specifies otherwise, in case of the recording of audio or photographic material in a public space, for the purpose of publicizing it, the consent of the data subject shall be replaced with the notification of the data subject in a form which enables him / her to acknowledge the fact of recording and to prevent himself / herself from being recorded. The notification obligation does not exist in case of public events, when the recording of these events for publicizing purposes can be reasonably expected.
- Processing for the purposes of scientific or historical research purposes or for the purposes of official statistics – GDPR article 89. It is permissible to process personal data for these purposes without the data subject’s consent in pseudonymized form or in a form that ensures at least equivalent level of data protection. De-pseudonymization or other measure of changing non-identifiable personal data to identifiable personal data is only permissible for further research or official statistics. The processor must name the person, who has access to the data that enables de-pseudonymization.
    - The processing of personal data without data subject’s consent in a form that the data subject is identifiable is only permissible when:
        - Pseudonymization would make it impossible to achieve the purposes of data processing, or they would be impracticably difficult to achieve;
        - The processor believes that an overwhelming public interest exists;
        - Based upon the processed personal data, the amount of data subject’s obligations are not changed and data subject’s rights are not excessively damaged in any other way.

- Where the scientific research is based on special categories of personal data, the ethics committee or the DPI will ensure the fulfillment of these obligations.

Analyses and researches of government institutions, done for the purposes of policy making, is also considered scientific research according to the PDPA.

- The processor or controller is entitled to limit data subjects’ rights stated in GDPR articles 15, 16, 18, 21 only to the extent that the enforcement of these rights would probably make the achievement of scientific or historical research purposes, or the purposes of official statistics, impossible or obstruct it considerably.
    - Processing for archiving purposes in the public interest – GDPR article 89. The processor or controller is entitled to limit data subjects’ rights stated in GDPR article 15, 16, 18, 19, 20, 21 only to the extent that the enforcement of these rights would probably make the achievement of the purposes of archiving in the public interest impossible or obstruct it considerably. Limiting data subjects’ rights is permissible to protect the records, their authenticity, credibility, integrity and usability.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The PDPA and the Implementation Act do not foresee any derogations / additional requirements to the GDPR.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The PDPA and the Implementation Act do not foresee any derogations / additional requirements to the GDPR.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The PDPA and the Implementation Act do not foresee any derogations / additional requirements to the GDPR.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.

- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Estonian law does not recognize administrative fines. This is also reflected in Recital 151 of the GDPR, stating that since the Estonian legal system does not allow for administrative fines as set out in the GDPR, the rules on administrative fines may be applied in Estonia in such a manner that the fine is imposed in misdemeanor proceedings if the applicable rules allow for the imposition of fines that are effective, proportionate and decisive.

Under the PDPA, the DPI may impose fines in misdemeanor proceedings of up to 20,000,000 euros or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Nevertheless, Estonia has been among the EU Member States imposing the lowest GDPR fines across the EU. This has been due to constraints arising from misdemeanor procedural law, which has resulted in virtually no misdemeanor fines being imposed for GDPR violations. Currently, most infringements have been dealt with in state supervision proceedings (i.e. administrative proceedings) which does not allow for the imposition of fines.

With regard to administrative proceedings, the DPI may issue precepts to data controllers and processors to order them to stop the infringing activities.

Upon failure to comply with a precept of the DPI, DPI may impose a non-compliance levy pursuant to the procedure provided for in the Substitutional Performance and Non-Compliance Levies Act. The upper limit for a non-compliance levy is 20,000,000 euros or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Further, if the precept issued by the DPI is not fulfilled, the DPI may turn to a superior agency, person or body of the processor of personal data for organization of supervisory control or commencement of disciplinary proceedings against an official.

Against the background of constraints arising from misdemeanor procedural law described above, the Estonian legislator initiated, in 2019, a draft law amending the Penal Code (which is also applicable to misdemeanor proceedings), in order to allow for more effective and decisive implementation of fines as required under EU law. The new law has now entered into force (as of 1 November 2023). The main changes that are relevant for the GDPR enforcement are the following:

- the statute of limitations for misdemeanor offences resulting from breaches of the GDPR has been prolonged from 2 years (which was the case prior to 1 November 2023) to 3 years, enabling the DPI to investigate potential infringements for a longer time;
- the general part of the Penal Code now explicitly states that the upper threshold of 400,000 euros for misdemeanor fines will not apply if lex specialis foresees fines that are calculated on a different basis and in a different amount, allowing to impose higher misdemeanor fines than 400,000 euros. Prior to the legislative amendments, the Penal Code stated that the maximum misdemeanor fine that could be applied under law was 400,000 euros. The interplay between the referred provision as lex generalis and the provisions implementing the GDPR fines as lex specialis has been unclear to this date and has not been interpreted by the courts within more than the 5 years that the GDPR has been applicable (and in offence proceedings, i.e., misdemeanor and criminal proceedings, such discrepancies in law must be interpreted in a way that is favorable to the person under investigation);
- the general provision regarding a legal person’s misdemeanor liability now states that a legal person is held liable if an infringement has been committed either: (a) by any natural person according to instructions given by the legal person’s body, its member, a senior official or a competent representative; or (b) due to the insufficient work organization or lack of supervision by the legal person. It is also clearly stated in the law that if a

legal person is obliged to act under the law, the legal person is responsible for its inactions or omissions irrespective of whether or not a natural person was also obliged to act. Prior to the legislative amendments, the Penal Code stated that a legal person could be held accountable only for an act that was committed in the interest of the legal person by its body, a member thereof or by a senior official or competent representative. Meaning that in misdemeanor proceedings arising from breaches of the GDPR, the DPI had to identify a natural person who has acted in the interests of a legal person and that this natural person has committed an act that fulfils all the criteria of a punishable offence.

The respective legislative amendments now significantly simplify imposing fines on legal person. Fines can now be applied based on these rules for such GDPR infringements that have been committed from 1 November 2023 onwards or that have continued from 1 November 2023 onwards.

As a stand-alone aspect from the above, the PDPA further specifies that the DPI is entitled to apply certain special state supervision measures to carry out the necessary state supervision, in addition the DPI is entitled to use the measures specified in Article 58 of the GDPR. The DPI may make enquiries to electronic communications undertakings about the data required for the identification of an end-user related to the identification tokens used in the public electronic communications network, except for the data relating to the fact of transmission of messages, unless identification of an end-user is otherwise impossible.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg,* an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Electronic marketing is regulated by the Electronic Communications Act. As a general rule, the data subject must be able to consent to the electronic marketing. The requirements for this consent depend on whether the addressee is a natural or a legal person, and whether there is an existing client relationship between the parties. Real time non-automated phone calls and regular mail are not considered electronic marketing under Estonian law.

The customer consent must be obtained separately from other terms of the contract between the parties – i.e. it cannot be obtained in the standard terms presented to the customer (*eg,* 'By accepting these terms you agree to receive our commercial communications at the email address provided to us'). In practice, a checkbox separate from the acceptance of the standard terms is often used to obtain this consent.

An opt-in consent is required if the addressee is a natural person, except in the case of an existing client relationship, where opt-out is permissible. The message itself must always include information to clearly determine the person on whose behalf the marketing is sent, clearly distinguishable direct marketing information and clear instructions on how to refuse to receive further direct marketing (*eg,* an unsubscribe link).

Reliance on an opt-out (for natural persons) in the framework of existing client relationships is subject to the following additional requirements:

- the same entity has obtained the contact details in the course of a sale;
- the direct marketing is in respect of similar goods or services;
- the recipient was given a possibility to opt out at the collection of his / her personal data;
- the message must include information to clearly determine the person on whose behalf the marketing is sent; and
- the message must include clearly distinguishable direct marketing information and the recipient is given a simple means in each subsequent email to opt out/unsubscribe.

If the addressee is a legal person, the opt-out system is applicable. There is no need to obtain a prior consent for direct marketing, but:

- the message must include information to clearly determine the person on whose behalf the marketing is sent;
- the message must include clearly distinguishable direct marketing information; and
- the recipient is given a simple means in each subsequent email to opt out / unsubscribe.

ONLINE PRIVACY

Traffic data and location data

Traffic data retention requirements apply only to communications undertakings. Providers of telephone or mobile telephone services and telephone network and mobile telephone network services, as well as providers of Internet access, electronic mail and Internet telephony services are required to preserve for a period of one year network traffic data, location data and associated data thereof which is necessary to identify the subscriber or user in relation to the communications services provided.

Cookies

Due to the opt-out system, consent to cookies is not needed. The law does not refer specifically to browser settings or other applications to be adopted in order to exercise the right to refuse.

The PDPA specifies, that if GDPR article 6(1)(a) is used with regard to providing information society services directly to a child, then the processing of the child’s personal data is permitted if the child is at least 13 years old. If the child is younger, then processing is permissible only if and in the extent to which the child’s legal representative has agreed to.

KEY CONTACTS

Sorainen
www.sorainen.com/

Kaupo Lepasepp
Partner
Sorainen
T +372 6 400 939
kaupo.lepasepp@sorainen.com

Mihkel Miidla
Partner, Head of Technology & Data Protection
Sorainen
T +372 6 400 959
mihkel.miidla@sorainen.com

Liisa Maria Kuuskmaa
Senior Associate
Sorainen
T +372 6 400 900
liisa.kuuskmaa@sorainen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ETHIOPIA

Last modified 12 January 2023

LAW

Ethiopia has several laws that relate to privacy and data security, including:

- The 1995 Constitution of the Federal Democratic Republic of Ethiopia;
- Tthe 2005 Criminal Code of the Federal Democratic Republic of Ethiopia:
- The 1960 Civil Code, the Computer Crime Proclamation No. 958/2016;
- Freedom of the Mass Media and Access to Information Proclamation No. 590/2008 (as amended by the Media Proclamation No. 1238/2021);
- Federal Advocacy Service Licensing and Administration Proclamation No.1249/2021;
- Telecom Fraud Offence Proclamation No. 761/2012;
- Registration of Vital Events and National Identification Cards Proclamation No. 760/2012 (as amended);
- Federal Tax Administration Proclamation No.983/2016;
- Authentication and Registration of Documents' Proclamation No.922/2015;
- Electronic Signature Proclamation No.1072/2018;
- Communications Service Proclamation No.1148/2019;
- Electronic Signature Proclamation No.1072/2018;
- Electronic Transaction Proclamation No.1205/2020;
- National Bank of Ethiopia (NBE) Licensing and Authorization of Payment Instrument Issuers Directive No. ONPS/01/2020;
- NBE Financial Consumer Protection Directive No. FCP/01/202

DEFINITIONS

Definition of Personal Data

No specific definition is generally applicable.

The Freedom of the Mass Media and Access to Information Proclamation No. 590/2008, applicable to government entities, is understood to generally define personal data as information about an identifiable individual that relates, but is not limited, to:

- medical, education, academic, employment, financial transaction, professional or criminal history
- ethnic, national or social origin, age, pregnancy, marital status, color, sexual orientation, physical or mental health, well-being, disability, religion, belief, conscience, culture, language or birth
- an identification number, symbol or other identifier assigned to the individual, address, fingerprints or blood type
- personal opinions, views or preferences, except as relate to another individual
- views or opinions on grant proposals, awards, or prizes granted to another individual, provided such views or opinions are not associated with the other individual’s name
- views or opinions of others about the individual, or

- an individual’s name, in combination with other personal data, or alone, if could reasonably be linked to personal data (exception applies for persons deceased for more than 20 years).

Ethiopian Communications Authority’s Consumers Rights and Protection Directive 2020 defines personal information as private information and record relating to consumers leading to identify such consumer such as his identity, address or telephone number and / or traffic and billing data and / or other personal information.

Definition of Sensitive Personal Data

Sensitive personal data is not defined.

NATIONAL DATA PROTECTION AUTHORITY

There is no data protection authority.

REGISTRATION

There is no requirement to register databases or personal data processing activities.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

Though Ethiopia has not enacted a specific law to address personal data collection and processing issues, the country’s scattered legislative framework is understood to require that personal data be collected and processed with due care and only for an intended lawful purpose. Obtaining express consent for collecting and processing of personal data is also a requirement under those scattered provisions.

TRANSFER

No specific geographic transfer restrictions apply in Ethiopia.

However, existing law provides that personal data transfers must be based on the prior written consent of the person whose data is to be transferred and only for an intended lawful purpose.

SECURITY

There are no specific data security requirements.

The Computer Crime Proclamation No. 958/2016 requires service providers to implement reasonable and necessary security measures to protect confidential computer traffic data disseminated through their computer systems or communications services from unlawful and unnecessary access.

Ethiopian Communications Authority’s Sim Card Registration Directive requires Telecommunication Operators to take all reasonable steps to ensure the security and confidentiality of its subscribers’ registration details.

BREACH NOTIFICATION

There is no general breach notification requirement in Ethiopia.

However, the Computer Crime Proclamation No. 958/2016 requires service providers with knowledge that a crime stipulated by the Proclamation (including breach of privacy via unauthorized access) has been committed by a third party through the computer system it administers to immediately notify the Information Network Security Agency, report the crime to police, and take appropriate measures.

Ethiopian Communications Authority’s Sim Card Registration Directive under Article 24 obliges a telecommunication operator to notify the Ethiopian Communications Authority of any data breach that compromises subscribers’ information within seven (7) business days from discovery of the breach. The operator shall also notify the affected subscriber of such breach.

ENFORCEMENT

Ethiopian courts are responsible for enforcing data protection and privacy provisions in the law.

ELECTRONIC MARKETING

Electronic Transaction Proclamation No.1205/2020 backed by Electronic Signature Proclamation No.1072/2018 regulate aspects of electronic marketing in addition to general contract law and commercial law provisions.

ONLINE PRIVACY

There are several provisions in Ethiopian law to regulate online privacy. For example, the Computer Crime Proclamation No. 958 /2016 criminalizes the unauthorized access to, and illegal interception and damage of, computer data.

The Proclamation further prohibits the use of computer systems to disseminate advertisements absent addressee consent.

The new Media Proclamation obliges online Media to protect the data of users and obtain explicit consent from users when circumstances requiring users’ data to be made available to third parties.

KEY CONTACTS

Benyam Tafesse
Head, Employment, IP & Aviation Practices
Mehrteab Leul & Associates
T +251 115 159 798
benyam@mehrteableul.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

FEDERATED STATES OF MICRONESIA

Last modified 31 January 2023

LAW

There are no data protection laws or statutes outside of the telecommunications context. The relevant text is the Federated States of Micronesia Code (“**FSM Code**”).

DEFINITIONS

None.

NATIONAL DATA PROTECTION AUTHORITY

None.

REGISTRATION

None.

DATA PROTECTION OFFICERS

None.

COLLECTION & PROCESSING

Sections 349 and 350 of Title 21 of the FSM Code obligate telecommunications providers to ensure the confidentiality of customer information and communications.

21 F.S.M.C. 349 precludes the collection, use, maintenance or disclosure of information about a customer for any purpose without the customer’s consent and mandates application of appropriate security safeguards to prevent such collection, use, maintenance or disclosure of information without consent.

TRANSFER

None.

SECURITY

None.

BREACH NOTIFICATION

None.

ENFORCEMENT

None.

ELECTRONIC MARKETING

None.

ONLINE PRIVACY

None.

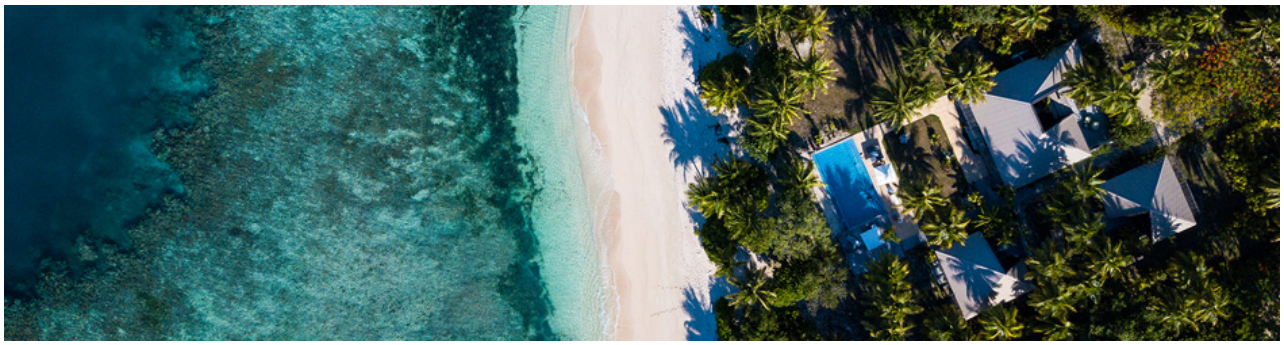
KEY CONTACTS

Michael J. Sipos, Esq.
Attorney at Law
Pacific Lawyers
T 691-320-6450
msipos@mail.fm

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

FIJI



Last modified 3 January 2024

LAW

There is no specific legislation for personal data protection in Fiji. Clause 24 of the Constitution (2013) provides the right to personal privacy, includes right to confidentiality of personal information.

Some sector-specific laws criminalise (or expose to other serious action) the unauthorised disclosure by others of personal / client information as follows:

- Banking Act 1995 – by central bank personnel (s.27) and licensed financial institution personnel (s.71);
- Fiji Revenue and Customs Service Act 1998 – by tax officials (s.52 (2));
- Medical and Dental Practitioner Act 2010 – by statutory administrators of any data obtained in the course of their duties (s.126);
- Under the Rules of Professional Conduct and Practice (para 1.4) of the Legal Practitioners Act 2009 - information received by legal practitioners from or on behalf of clients;
- Cybercrime Act 2021 defines "computer data" which is broad enough to capture personal data if it is stored in a computer system.

These laws, however, do not directly protect personal information.

DEFINITIONS

Definition of Personal Data

The only actionable rights available to citizens are in s.24 of the Constitution. This creates a right to “personal privacy”, said to include:

- “confidentiality of their personal information;
- confidentiality of their communications; and
- respect for their private and family life”.

These terms are not otherwise defined.

Definition of Sensitive Personal Data

None.

NATIONAL DATA PROTECTION AUTHORITY

None.

REGISTRATION

None.

DATA PROTECTION OFFICERS

None.

COLLECTION & PROCESSING

No applicable laws.

TRANSFER

No applicable laws.

SECURITY

No applicable laws.

BREACH NOTIFICATION

No applicable laws.

ENFORCEMENT

No applicable laws.

ELECTRONIC MARKETING

No applicable laws.

ONLINE PRIVACY

No applicable laws.

KEY CONTACTS

Munro Leys
www.munroleyslaw.com/

Richard Naidu
Partner
Munro Leys
T +679 322 1816
richard.naidu@munroleyslaw.com.fj

Bhumika Khatri
Senior Associate
Munro Leys
T +679 322 1824
bhumika.khatri@munroleyslaw.com.fj

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

FINLAND

Last modified 4 January 2023

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

Finland has passed a supplementary implementation act of the GDPR, the Data Protection Act of Finland *(Tietosuojalaki)*, which entered into force on January 1, 2019.

Other key Finnish laws concerning data privacy and protection are: the Act on Electronic Communication Services 917 /2014 *(Laki sähköisen viestinnän palveluista)* of January 1, 2015, which aims to, inter alia, ensure the confidentiality of electronic communication and the protection of privacy; the Act on the Protection of Privacy in Working Life 759/2004 (‘Working Life Act’) *(Laki yksityisyyden suojasta työelämä ssä),* which aims to promote the protection of privacy and other rights safeguarding the privacy in working life, and; the Act on the Processing of Personal Data in Criminal Cases and in connection with Maintaining National Security 1054 /2018 *(Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä*), which entered into force on January 1, 2019 along with the Data Protection Act.

The Working Life Act includes some specific provisions on privacy issues relating to employment and work environments such as right to monitor employees’ email communication. The protection of employees’ privacy has traditionally been strict in Finland and Finland uses the national leeway provided in the GDPR with regard to processing of personal data in the context of employment and maintains the specific law concerning privacy in working life.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions in Finland are the same as in the GDPR and no additional local definitions have been included.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

In Finland The Office of the Data Protection Ombudsman (*Tietosuojavaltuutetun toimisto*) is the local supervisory authority. The Office of the Data Protection Ombudsman contains the Data Protection Ombudsman himself, two Assistant Data Protection Ombudsmen as well as various data protection experts and secretaries as public servants.

Post address: P.O. Box 800, 00531 Helsinki Finland

Visiting address: Lintulahdenkuja 4, 00530 Helsinki Finland

T +358 29 56 66700

tietosuoja@om.fi

www.tietosuoja.fi

The Data Protection Act specifies the Data Protection Ombudsman’s duties and rights under the GDPR regarding *e.g.,* audits, right to receive information and right to impose sanctions on entities.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

The Finnish Data Protection Act does not contain any provisions related to registration. The former Finnish Personal Data Act did contain some requirements for registration, but these have been repealed.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

In Finland the new Data Protection Act does not contain specific local requirements on data protection officers. However, few special national acts stipulate mandatory appointment of data protection officers.

For example, in Finland all functional units of healthcare and social welfare as well as pharmacies must appoint a data protection officer under the Act on Electronic Prescriptions 2007/61 *(Laki sähköisestä lää kemääräyksestä),* and under The Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (159/2007) *(Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä kä sittelystä)*.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;

- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)

- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Finland has used the national leeway provided in GDPR article 6(1) subsection e) as well as GDPR article 9(2) subsections b), g), h), i) and j) regarding collecting and processing personal data in certain situations.

In Finland, personal data may be processed under GDPR article 6(1) e) when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, if:

it relates to information representing a person’s position, tasks and the processing thereof in the public sector entity, business life or other equivalent activity, the purpose of processing rests on the public interest grounds and it complies with the principle of proportionality;

- it is necessary in the operation of authorities in order to perform a task in public interest and it complies with the principle of proportionality;
- it is necessary for scientific or historical research or statistical purposes and it complies with the principle of proportionality; or
- the processing of research material, material related to cultural heritage and any description information thereof for archiving purposes is necessary on public interest grounds and complies with the principle of proportionality.

The processing of special categories of personal data under GDPR article 9(2) subsections b), g), h), i) and j) may be carried out in Finland if it concerns, by way of example:

- personal data of the insured person or a claimant within the operation of an insurance company to settle its liability;
- health and medical data in connection with certain operations of healthcare and social welfare service providers; or
- processing for scientific or historical research purposes or statistical purposes.

In addition to the above-mentioned processing activities, the national leeway has also been used in the Data Protection Act with respect to processing related to criminal convictions and offences as well as processing of national identification numbers. For example in relation to national identification numbers, processing is only allowed based on data subject consent or if it is necessary to unambiguously identify the data subject for: a) a task defined in law, b) realization of the rights and responsibilities of the data subject or data controller, or c) historical or scientific research or statistical purposes. Further, national identification numbers can be processed for e.g. credit, loan, insurance, debt collection, payment service and leasing purposes, in social or healthcare services, and in connection with employment relatioships.

The Working Life Act sets additional processing requirements to employment related data that an employer collects and processes of its employees. All employee personal data processed must at all times be directly necessary for the employee’s employment relationship. This necessity requirement cannot be bypassed even with the employee’s consent.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defense of legal claims;

f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The new Data Protection Act does not include additional clauses concerning transfer of personal data, *ie,* Finland has decided not to use the marginal national leeway provided in GDPR articles 46 and 49 as per now.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The new Finnish Data Protection Act does not contain any direct additional requirements for the security of processing in the meaning of GDPR article 32. However, the Data Protection Act does specify the security measures to be taken if special categories of personal data are processed. These measures are mostly the same as included in the GDPR article 32 (*eg,* pseudonymization, encryption, personnel training, access management, log-on data usage), and according to the government proposal explanatory text serve more as examples of what measures must be taken rather than an exhaustive mandatory list despite the wording used.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

In Finland the general breach notification procedure follows the rules set by GDPR.

Personal data breaches must be reported to the Office of the Data Protection Ombudsman. The report can be made to the Office of the Data Protection Ombudsman through their website.

However, certain special national legislation does include additional requirements on breach notifications. The Act on Electronic Communication Services establishes an obligation for telecommunications operators to notify their subscribers, users and the Finnish Transport and Communications Authority (‘*Traficom*’) of significant information security violations or threats and of anything else that prevents or significantly interferes with communication services. In addition, under the Act on Electronic Communication Services, domain name registrars shall notify *Traficom* without undue delay of significant violations of information security in its domain name services and of anything that essentially prevents or disturbs such services.

The Act on Strong Electronic Identification and Electronic Signatures (2009/617) (*Laki vahvasta sähkö isestä tunnistamisesta ja sähköisistä luottamuspalveluista*) also states that an electronic identification service provider shall notify service providers using its services, identification device holders as well as *Traficom* of severe risks and threats to its data security.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will

need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

In Finland, the Data Protection Ombudsman and the Deputy Data Protection Ombudsmen supervise compliance with GDPR and the Finnish Data Protection Act. In addition, an Expert Committee provides statements on significant questions and matters related to data processing upon the request of the Data Protection Ombudsman.

The Data Protection Ombudsman may order a data controller or data processor to comply with certain articles of the GDPR as well as Section 18 of the Data Protection Act, which covers the Data Protection Ombudsman’s right to receive necessary information, and impose a default fine to make the order more effective. However, the default fine may not be imposed on a natural person due to them not complying with the section on the Data Protection Ombudsman’s right to receive information if the person is suspected of a crime and the information is related to the alleged crime.

Administrative fines defined in article 83 of the GDPR will be issued by a sanction board within the Office of the Data Protection Ombudsman. The sanction board consists of the Data Protection Ombudsman and the two Deputy Data Protection Ombudsmen and the decision shall be made as a majority decision. Finland has decided to use the provided national leeway and the Act regulates that the administrative fines cannot be issued to:

- state authorities;
- state-owned businesses;
- local authorities;
- independent public institutions;
- organs operating in connection with the Parliament;
- the Office of the President of the Republic; or
- the Evangelical Lutheran Church of Finland or the Orthodox Church of Finland or the parishes, associations of parishes or other bodies thereof.

In addition, criminal sanctions can ensue from breaches of data protection laws in Finland as the Criminal Code of Finland 39/1889 (*Rikoslaki*) includes several data processing, data privacy, confidentiality and data security related offences or crimes. Finland has also introduced a punishable offence, the data protection offence, to the Criminal Code of Finland based on the GDPR. If the controller or data processor commits a data protection offence, the punishment is a fine or up to one year of imprisonment. The Criminal Code also states that the prosecutor is obligated to hear the Data Protection Ombudsman before bringing charges against a controller or data processor for a data protection offence.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Act on Electronic Communication Services regulates direct marketing by electronic means in Finland. The Data Protection Ombudsman is the supervising authority also in compliance issues with the Act on Electronic Communications Services’ provisions concerning direct marketing.

Direct marketing to natural persons is only allowed by means of automated calling systems, facsimile machines, or email, text, voice, sound or image messages and only if the natural person has given his / her prior consent to it. Direct marketing using other means is allowed if the natural person has not specifically forbidden it. If, however, a service provider receives an email address, number or other contact information in relation to the sale of product or service, the service provider may normally use this contact information to directly market the service providers own products or services belonging to the same product group or that are otherwise similar to the natural person in question. The natural person must be able to easily and at no charge unsubscribe from or prohibit any direct marketing and the service provider must clearly inform the natural person of that possibility.

A service provider may use direct marketing with legal persons (businesses) unless they have specifically prohibited it. As with natural persons, legal persons must also be able to easily and at no charge unsubscribe from/prohibit any direct marketing and the service provider must clearly inform the legal person of that possibility. In addition, telecommunications operators and corporate or association subscribers are entitled, at a user’s request, to prevent the reception of direct marketing.

The Data Protection Ombudsman and the Finnish Customer Marketing Association have given their interpretations on B2B direct marketing using a legal person’s general contact information, such as an email address (e.g. info@company.com). If the B2B direct marketing is sent to a legal person’s employee’s personal work email (fistname.lastname@company.com), the person’s prior consent is required unless the marketed product or service is substantially related to the person’s work duties based on the person’s job description.

Email, text, voice, sound or image message sent for the purpose of direct marketing must be clearly and unmistakably be recognized as direct marketing. It is forbidden to send such a direct marketing message that:

- disguises or conceals the identity of the sender on whose behalf the communication is made;
- is without a valid address to which the recipient may send a request that such communications be ended;
- solicits recipients to visit websites that contravene with the provisions of the Consumer Protection Act 20.1.1978 /38 (*Kuluttajansuojalaki*).

If any processing of personal data is involved in the electronic direct marketing, the provisions of the applicable data protection laws (such as the Finnish Data Protection Act and the GDPR) will also apply.

ONLINE PRIVACY

The Act on Electronic Communication Services 917/2014 *(Laki sähköisen viestinnän palveluista)* regulates online privacy matters such as the use of cookies and location data.

Cookies

A service provider is allowed to save cookies and other data in a user’s terminal device, as well as use such data, only with the consent of the user. The service provider must also give the user clear and complete information on the purposes of use of cookies.

However, the above restrictions do not apply to use of cookies only for the purpose of enabling the transmission of messages in communications networks or which is necessary for the service provider to provide a service that the subscriber or user has specifically requested.

In April 2021, Helsinki Administrative Court ruled in its decision that the competent supervisory authority in cookie consent issues is Transport and Communications Agency Traficom, not the Office of the Data Protection Ombudsman. However, the Office of Data Protection Ombudsman remains competent supervisory authority in other cookie matters.

Traficom published in September 2021 a guideline “Instructions for service providers” updating its instructions on cookie implementation on consent collection. For consent to meet the requirements set in the GDPR, users must have the

opportunity to choose whether to accept or reject the terms offered. Consent can be given in a variety of ways, as long as it clearly indicates that the data subject accepts the proposal for the processing of their personal data. Valid consent cannot be given through silence, pre-ticked boxes or inactivity. Refusing and withdrawing consent must be as easy as giving consent. The controller must also be able to demonstrate the consent afterwards.

Location Data

The location data associated with a natural person can be processed for the purpose of offering and using added value services, if;

- the user or subscriber, whose data is in question, has given his / her consent;
- if the consent is otherwise clear from the context; or
- is otherwise provided by law.

In general, location data may only be processed to the extent necessary for the purpose of processing and it may not limit the privacy any more than absolutely necessary.

The added value service provider shall ensure that:

- the user or subscriber located has easy and constant access to specific and accurate information on his / her location data processed, purpose and duration of its use and if the location data will be disclosed to a third party for the purpose of providing the services:
- the above mentioned information is available and accessible to the user or subscriber prior him / her giving his/her consent;
- the user or subscriber has the possibility to easily and at no separate charge cancel the consent and ban the processing of his / her location data (if technically feasible).

The user or subscriber is entitled to receive the location data and other traffic data showing the location of his/her terminal device from the added value service provider or the communications provider at any time.

KEY CONTACTS

Markus Oksanen
Partner
T +358 9 4176 0431
markus.oksanen@fi.dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

FRANCE

Last modified 19 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (“GDPR” or ”**Regulation**”) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. This is the “*establishment criterion*”. An 'establishment' may take a wide variety of forms and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behavior*" (Article 3(2)(b)) as far as their behavior takes place within the EU. This is the “targeting criterion”.

France updated Law No. 78-17 of January 6, 1978 on information technology, data files and civil liberties (the “**Law** ”) to GDPR with the enactment of (i) Law No. 2018-493 of June 20, 2018 on the protection of personal data, and (ii) Order No. 2018-1125 of December 12, 2018, adopted pursuant to Article 32 of Law No. 2018-493, updates the Law and other French laws relating to personal data protection in order to “simplify the implementation and make the necessary formal corrections to ensure consistency with EU data protection law”. France domestic data protection legislation was further completed with the adoption of Decree No. 2019-536 of May 29, 2019, adopted for the application of the Law (the “**Decree**”). The Decree clarifies procedural rules of the French data protection authority, including its control and sanctions, and further specifies data subject rights.

The Law and the Decree have been updated:

- in 2021, (i) Law No. 2021-988 of July 30, 2021, on the prevention of acts of terrorism and intelligence amended articles 48 and 49 of the Law to create exceptions to the rights of individuals when processing is justified by national security and (ii) Law No. 2021-1017 of August 2, 2021, relating to bioethics which modified article 75 of the Law relating to processing in the health field; and

- in 2022, (i) Law No. 2022-52 of January 24, 2022, on criminal liability and homeland security amends articles 10, 20, 125 of the Law and created article 22-1 to introduce the simplified sanction procedure of the French data protection authority and (ii) Decree No. 2022-517 of April 8, 2022, amends the Decree to define the modalities of this simplified sanction procedure as introduced by Law No. 2022-52 of January 24, 2022. The objective of these new texts is to introduce more flexibility in the use of formal notices or sanctions.

Territorial Scope

As of today, Article 3 of the Law provides that it applies when (i) the data controller or data processor is established in France (whether the processing takes place in France or not) or (ii) the data subjects reside in France (for the possible legal variations as permitted from time to time of the GDPR. Contrary to the GDPR, the Law has not included the “targeting criterion”.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions under the Law are the same as under the GDPR. Article 2 of the Law makes an express reference to GDPR definitions, thus harmonizing the definitions and concepts of French law with the GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the CNIL in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single

establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The « *Commission Nationale de l’Informatique et des Libertés* » or « CNIL » is the French supervisory authority

Address

3 place de Fontenoy
TSA 80175
75334 Paris Cedex 07

Telephone

01 53 73 22 22

Website

cnil.fr

The CNIL has different missions and powers, which mainly include:

i. informing data subjects and data controllers / processors (whether public or private) about their rights and obligations;
ii. ensuring compliance of all personal data processing with French and EU data protection rules as well as data protection rules resulting from international commitments of France;
iii. anticipating new challenges and issues arising from innovation and the use of new technologies, including privacy in general and ethics;
iv. controlling and sanctioning.

In addition, the Law provides for mutual assistance and joint operations with other EU Supervisory Authorities, as well as cooperation with non-EU supervisory authorities.

The CNIL has a range of tools to complete its missions including e.g., publication of reference frameworks created after consultations with the stakeholders or sectors at hand, among which standard regulations (which are mandatory in respect of processing of biometric, genetic, health or criminal convictions and offences data), reference methodologies in the sector of health, guidelines, recommendations and standards, approval of codes of conduct and certifications, broad range of on-site and off-site investigation powers and sanctions. The Law provides further precisions on the functioning of the CNIL and its specific tasks and powers, notably the extent of on-site investigations and procedural requirements, in connection with the missions described above.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or

processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Prior formalities with the CNIL are no longer required and are replaced by the obligation to hold a record of processing which include the same categories of information as those initially requested in the filing forms.

However, formalities are maintained for the processing of data in the health sector which is subject either to a declaration of conformity to specific requirements defined by the CNIL or an authorization by the CNIL. In this respect, the CNIL has issued eight (8) methodologies of reference ("*Methodologies de Reference*" or "MR") for various types of research in the health sector. A formal commitment to comply with these methodologies exempts the data controller – generally the sponsor of the research – from having to apply for a formal authorization with the CNIL.

Certain specific processing of personal data must be authorized by decree of the State Council (*Conseil d’Etat*) or ministerial order, taken after a motivated and public opinion of the CNIL. These processing are as follows:

- Processing of the social security number (with a few exceptions);
- Processing carried out by or on behalf of the State, acting in the exercise of its public authority prerogatives, of genetic or biometric data necessary to the authentication or identity control of individuals;
- Processing carried out on behalf of the State (i) which concern State security, defense, national security, or (ii) which purpose is the prevention, investigation, detection or prosecution of criminal offences, or enforcement of criminal convictions or security measures.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope, or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;

- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Law provides that controllers processing personal data under the scope of the EU Data Protection Directive on Police and Criminal Justice Cooperation must appoint a DPO, with the exception of jurisdictions acting within the scope of their judicial activity.

The Decree specifies the mandatory information to be communicated to the CNIL by data controller(s) or processor(s) in the DPO notification form.

On 20 September 2018, the CNIL issued two standards regarding the certification of DPO skills: one regarding the skills and know-how expected to be certified as DPO (CNIL Deliberation No. 2018-318), and the other one regarding the criteria applicable to certifying DPO organizations (CNIL Deliberation No. 2018-317). These Deliberations were recently updated notably to adapt the procedure of accreditation of the organizations authorized to certify the DPOs’ skills and to enable candidates to take the certification test remotely (CNIL Deliberation No. 2022-128 and CNIL Deliberation No. 2023-062).

On March 2022, the CNIL also published a Guide for DPOs that combines useful knowledge and best practices to help organizations in appointing and supporting DPOs.

COLLECTION & PROCESSING

Data protection principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal basis under article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special category data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 legal basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal convictions and offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a secondary purpose

Increasingly, organizations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (privacy notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the data subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Special category data

The Law contains specific provisions regarding the processing of health data (e.g. see above regarding authorization requirements), as well as additional provisions regarding processing of special categories of personal data.

Criminal convictions and offences data

The following categories of persons can process such personal data:

- Courts, public authorities and legal persons entrusted with a public service, acting within the scope of their legal functions, as well as entities collaborating with judicial entities as listed in the Decree;
- Auxiliaries of justice, for the strict exercise of their functions;
- Individuals and private entities to prepare, bring or defend a claim in court as a victim or defendant, and to execute the court decision, for the duration strictly necessary for these purposes. It is possible to share such information with third parties under the same conditions and for the same purposes;
- Collective IP rights management organizations for the purpose of defending those rights; and
- Persons reusing public information appearing in published rulings, provided that the processing has neither the purpose or effect of allowing the re-identification of the concerned persons.

In addition, the following categories of persons are authorized by the Decree to process personal data relating to criminal convictions, offenses or related security measures:

- Victims support associations contracted by the Ministry of Justice;
- Associations of assistance to the reintegration of persons placed under the authority of justice, in the respect of their social object;
- The establishments mentioned in 2 ° of I of Article L. 312-1 of the Code of Social Action and Families as part of their mission of medico-social support;
- The establishments and services mentioned in 4 ° and 14 ° of I of Article L. 312-1 of the Code of Social Action and Families;
- The drop-in and reception centers mentioned in III of Article L. 312-1 of the Code of Social Action and Families; The medical or medico-educational establishments authorized mentioned in articles 15 and 16 of the order No. 45-174 of 2 February 1945 relating to delinquent childhood;
- The public or private educational or vocational training institutions, authorized and appropriate boarding schools for juvenile school-aged offenders mentioned in Articles 15 and 16 of the aforementioned order of 2 February 1945;
- Private legal entities exercising a public service mission or the authorized associations mentioned in Article 16 of the aforementioned order of 2 February 1945;
- The legal representatives for the protection of the adults mentioned in Article L. 471-1 of the Code of Social Action and Families.

The CNIL may issue standard regulations, prescribe additional measures to be implemented, including of a technical and organizational nature, and / or complementary warranties for processing of special categories of data, including notably criminal convictions and offences data, by public and private entities (except for processing carried out in connection with the exercise of public authority by or on behalf of the State).

In addition, processing of criminal convictions and offences data which purpose is the prevention, investigation, detection or prosecution of criminal offences, or enforcement of criminal convictions or security measures by or on behalf of the State is subject to an order of the competent Ministry.

Transparency (privacy notices)

The Law mandates data controllers to provide data subjects with information relating to their right to define directives relating to the processing of their personal data after their death (digital legacy).

In addition, where the data is collected from a data subject under 15, the data controller must provide the mandatory information provided for by Art. 13 GDPR in a clear and easily accessible language.

The French data subjects should be also provided with the information relating to the processing of their personal data in French (notably in accordance with Act no. 94-665 dated 4 August 1994 related to the use of the French language).

Rights of the data subjects

The Decree describes the conditions in which the data subjects can exercise their rights (and more precisely, the conditions to check the identity of the data subject making the right request).

Data subjects’ rights can be restricted notably to avoid obstructing administrative investigations, inquiries or procedures, to safeguard the prevention, investigation, detection and prosecution of criminal offences, as well as of administrative enquiries, or to protect the rights and freedoms of others.

Digital legacy

Data subjects have the right to give instructions regarding the storage, deletion and communication of their personal data after their death (Articles 48 and 85 of the Law). Such instructions can be either:

- General, in which case they apply to all their personal data, irrespective of who the controller is. Such instructions can be given to a trusted third party certified by the CNIL; however, the implementing decree in this respect has never been adopted since the adoption of this provision in 2016; or
- Specific to one or several services, in which case the data subject can also give his / her instructions to the relevant data controller. It is required to obtain the specific consent of the data subject, and such consent cannot derive from his/her consent to general terms and conditions.

If the data subject has not given any instructions in his / her lifetime, then his / her heirs can exercise certain rights, in particular:

- The right of access, if it is necessary for the settlement of the succession; and
- The right to close the deceased’s accounts and to cease the processing of his / her personal data or, request the update of the personal data of the deceased.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay, New Zealand, Japan, the United Kingdom, the Republic of Korea and the United States (for companies certified under the EU-US Data Privacy Framework).

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules and standard contractual clauses. Controllers should also take additional requirements provided by the EDPB Recommendations 01/2020, following-up to the CJUE Schrems II Decision, i.

e., Transfer Impact Assessment and where necessary, supplementary measures. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defense of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

In the event processing of personal data involves a transfer of data outside the European Union territory, data subjects must be provided with mandatory information on, inter alia, the data transferred, the purpose of the transfer, the recipients of the data and the transfer mechanism used in accordance with the GDPR.

With respect to transfers made on the basis of Article 49(1)§2 of GDPR ("compelling legitimate interest"), the Decree provides that the CNIL will define templates (including annexes) to be used by data controllers to inform the CNIL about such transfers.

With respect to transfers made on the basis of code of conduct or other certification mechanism approved by the CNIL in accordance with the Law and the Decree, the Decree provides that data controller / data processor that rely on such transfer mechanisms shall provide the CNIL with a binding and enforceable commitment to apply appropriate safeguards to data subjects’ rights and freedoms in the concerned third-country.

For more information, please visit our Transfer – global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Although there is no specific requirements other than those set forth in the GDPR, the CNIL and the French Cyber Security Agency (“ANSSI”) have issued security guidance and recommendations containing state-of-the-art security practices, in particular: the 2023 version of the Personal Data Security Guide and the 2022 version of the recommendations on password and other shared secrets.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

Article 85 of Decree restricts the obligation of notification under Article 34 of the GDPR for the following processing:

- Processing including personal data allowing to identify, directly or indirectly, individuals whose identity is protected under Article 39 sexies of the French law on the freedom of the press; and
- Administrative, financial and operational data, as well as health data processing for which the notification of an unauthorized disclosure or access is likely to result in a risk for the national security, defense or public, due to the volume of data affected by the breach and the private information it contains (such as the family address or composition).

The Law provides that a Decree by the State Council, adopted after seeking the CNIL’s opinion (yet to be adopted) will specify a list of categories of processing and processing operations that derogate to the data breach notification requirement. Such derogation will only apply to processing that are necessary pursuant to a legal obligation bearing on the data controller or a public interest mission vested in the data controller, where such data breach notification would likely result in a risk to homeland security, defense or public safety.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

> For instance, in France, criminal penalties which can go up to 5 years of prison and EUR 300,000 fine for natural persons and EUR 1,500,000 for legal persons.

In May 2023, the EDPB issued Guidelines 04/2022 on the calculation of administrative fines under the GDPR.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Since 24 January 2022, the CNIL can investigate and use corrective powers following the simplified sanction procedure (Article 22-1 of the Law). This accelerated procedure can be used when a case does not present a specific issue (e.g. there is an established case law on the issue, the factual and legal issues are considered as simple). In such case, the CNIL can pronounce one or more of the following measures: warning, injunction to bring the processing into compliance including a penalty payment of up to €100 per day of delay, and / or an administrative fine of up to €20,000. Sanction decisions issued pursuant to the simplified sanction procedure are not published.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Law does not contain explicit provisions with respect to electronic marketing. However, Article L. 34-5 of the French Postal and Electronic Communications Code regulates electronic marketing in France. The CNIL has issued guidelines on the basis of this provision.

The CNIL distinguishes between B2B and B2C relationships. In any event, all electronic marketing messages must specify the name of the advertiser and allow the recipient to object to the receipt of similar messages in the future.

Electronic marketing to consumers (B2C)

Electronic marketing activities are authorised provided that the recipient has given consent at the time of collection of his / her email address.

This principle does not apply when:

- the concerned individual is already a customer of the company and if the marketing messages sent pertain to products or services similar to those already provided by the company; or

> Note that the CNIL considers that the creation of an account does not prejudge the eventual ordering of products or services from the company. The CNIL considers that in the absence of a purchase, the company cannot purposefully invoke the benefit of the soft opt-in exception created by article L. 34-5 of the French Postal and Electronic Communications Code.

- the marketing messages are not commercial in nature.

In any event the concerned individual, at the time of collection of his / her email address, must be informed that it will be used for electronic marketing activities, and be able to easily and freely object to such use.

Electronic marketing to professionals (B2B)

Electronic marketing activities are authorized provided that the recipient has been, at the time of collection of his / her email address:

- informed that it will be used for electronic marketing activities, and
- able to easily and freely object to such use.

The message sent must relate to the concerned individual’s professional activity. Please note that email addresses such as contact@companyname.fr are not subject to the requirements of prior consent and the right to object.

ONLINE PRIVACY

Cookies

The EU Cookie Directive has been implemented in the Law. It states that any subscriber or user of electronic communications services must be fully and clearly informed by the data controller or its representative of:

- the purpose of any cookie (i.e. any means of accessing or storing information on the subscriber’s / user’s device, e.g. when visiting a website, reading an email, installing or using software or an app); and
- the means of refusing cookies,

unless the subscriber / user has already been so informed.

Cookies are lawfully deployed if the subscriber / user has expressly consented after having received information. Valid consent can be expressed via browser settings if the user can choose the cookies he / she accepts and for which purpose.

However, the foregoing provisions do not apply:

- to cookies the sole purpose of which is to allow or facilitate electronic communication by a user; or
- if the cookie is strictly necessary to provide online communication services specifically requested by the user.

Location and traffic data

The Postal and Electronic Communications Code deals with the collection and processing of location and traffic data by electronic communication service providers (CSPs).

All traffic data held by a CSP must be erased or anonymised. However, traffic data may be retained, for example:

- for the purpose of finding, observing and prosecuting criminal offences;
- for the purpose of billing and payment of electronic communications services; or
- for the CSP’s marketing of its own communication services, provided the user has given consent thereto.

Subject to exceptions (observing and prosecuting criminal offences; billing and payment of electronic communications services), location data may be used in very limited circumstances, for example:

- during the communication, for the proper routing of such communication; and
- where the subscriber has given informed consent, in which case the location data may be processed and stored after the communication has ended. Consent can be revoked free of charge at any time.

Cookies

The French Data Protection Supervisory Authority (CNIL) replaced its 2013 guidelines regarding cookies and trackers, which were no more compliant with the GDPR, by revised guidelines. Following the adoption of a version of its guidelines on cookies and other trackers on July 4, 2019, which have been partially annulled by a decision from the French highest administrative Court, the *Conseil d’Etat*, on 19 June 2020, the CNIL has adopted revised guidelines and the final version of its recommendations on the practical procedures for collecting consent concerning cookies and other trackers. The CNIL’s revised guidelines, adopted by way of deliberation No. 2020-091 of September 17th, 2020, are based on Article 82 of the Law, implementing Article 5 (3) of EU directive “ePrivacy”, into French law.

While the Revised Guidelines provide the CNIL’s guidance on how to read the relevant provisions of the French Data Protection Act, which governs the use of cookies and other trackers in France, the Recommendations adopted by a deliberation No. 2020-92 of September 17th 2020 provide practical guidance and examples to help professionals navigate the rules applicable to cookies and other trackers and comply with the requirements of Article 82 of the French Data Protection Act. These two documents constitute “soft law” and are not binding, but provide strong references for organizations to anticipate how the CNIL may conduct its compliance investigations.

Regarding consent, the CNIL has now specified that consent must be:

- **unambigous**: to align with the guidelines on consent issued by the Article 29 Working Party, the CNIL repeals its previous position according to which scrolling down, browsing or swiping through a website or app was considered as an acceptable expression of consent to cookies and allowed for cookies to be placed. Therefore, for the CNIL, continuing to navigate on a website or using an application is no more acceptable to evidence a consent to cookies. The absence of action from the user (i.e., no choice from the user) can no longer be construed as a valid consent but should rather be construed as refusal. This operates a shift from “soft opt-in” to active consent. The revised guidelines also outlines that pre-ticked boxes do not meet the GDPR standard of consent;
- **freely given**: the data subject must be able to exercise freely his / her choice. The CNIL has revised (albeit subtlety) its previous positioning regarding “cookie walls” (the practice of subjecting prior access to a website or application to the acceptance of cookies) – where the CNIL considered that consent could never be freely given when collected using cookie walls, the revised guidelines now specify that cookie walls are likely to hinder freely given consent. In addition, the CNIL has specified in its case law, that failure to provide a mean to refuse cookies “as easily” as it is to accept them (e.g., by way of dedicated buttons on a cookie banner) results in consent being not freely given, since users will lean toward accepting cookies rather than performing multiple clicks to refuse;

- **specific**: consent must be tailored to each purpose. Therefore acceptance of the general terms and conditions as a whole (“bundled” consent) does not constitute valid consent;
  informed: information to data subjects must be easily understandable by any of them. Information must be given in plain language. The use of complex technical or legal terms does not meet the requirement of prior information. Such information must at least include (i) the identity of the data controller(s) implementing the trackers (ii) a thorough list of the purpose(s) of the reading or writing operations (iii) the means available to consent or object to the use of cookies (iv) the consequences of accepting or refusing the use of cookies and (v) the right to withdraw consent;
- **evidenced**: all organizations that use cookies must implement appropriate mechanisms that allow them to demonstrate, at all times, that they have validly obtained consent from users. the revised guidelines specifically provide that users choices, be it consent or refusal, must be (i) clearly presented to users, notably as regards the available means to exercise such choice, (ii) collected and clearly evidenced (the recommendations give examples of how to ensure such evidence through the use of a consent management platform, screen capture, etc.) and (iii) recorded by data controllers, for an appropriate duration during which they would not ask the users again for their consent. Such duration may vary depending on the nature of the site or application concerned. According to the Recommendations, a good practice in that respect is 6 months – at the expiry of that term, controllers could ask users again to consent (or refuse) to the use of cookies and trackers; and
- **revocable**: organizations are encouraged to put in place user-friendly solutions to allow users to withdraw their consent as easily as they gave it. The CNIL highlights the fact that means to refuse cookies and trackers must be “as easy” as means available to accept use thereof. As a result, users must not be subjected to complex procedures for refusing cookies and trackers and withdraw their consent, which they must be able to do at any time. To that end, the CNIL provides practical examples and good practices in the Recommendations, from the use of a “reject all” button to the availability of a visible “cookies” icon enabling users to parameter their choices and withdraw their consent.

The updated guidelines do not provide a general rule regarding the data retention of cookies and the information collected via such cookies. The CNIL simply recommends that the user’s consent (or refusal) is renewed every 6 months. However, the CNIL has maintained, as guidance, the following data retention terms for certain analytics cookies that do not require users’ consent:

- the lifetime of these cookies should be limited to a period that allows a relevant comparison of audiences over time, as it is the case with a period of 13 months, and is not automatically extended for new visits;
- the information collected via these cookies is kept for a maximum period of 25 months; and
- the above-mentioned lifetimes and retention periods are periodically reviewed to ensure that they are limited to what is strictly necessary.

In course of 2021 and 2022, the CNIL undertook massive online investigations in order to check whether the organizations were compliant with the new guidelines. Further to said investigations, several formal notices have been sent to organizations from different sectors (major platforms of the digital economy, e-commerce companies, car rental companies, public service authorities, bank companies, etc.). The CNIL has also fined companies for non-compliance regarding the use of cookies. Heavy sanctions have been applied to GAFAM companies in particular, with administrative fines up to 90 million Euros for failures to comply with Article 82 of the Law. It is interesting to note that, in its decisions regarding cookies, the CNIL imposes its competence even in the presence of a Lead Authority appointed by the company sanctioned, on the ground that the French Supervisory Authority remains the competent authority to control compliance of the e-Privacy Directive requirements, which are specific rules prevailing on the general rules resulting from the GDPR where thus the “One Stop Shop” process does not apply. In March 2023, the CNIL announced that user tracking by mobile phones was a priority topic for its investigations in 2023. It indicated that it carried out several investigations on applications that access identifiers generated by mobile operating systems in the absence of user consent.

KEY CONTACTS

Denise Lebeau-Marianna
Partner
T + 33 (0)1 40 15 24 98
denise.lebeau-marianna@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

GABON

Last modified 8 January 2024

LAW

The data protection regime in Gabon is governed by the following laws and regulations:

- Act no. 025/2023 of 09/07/2023 amending Act no. 001/2011 of 25 September 2011 on the protection of personal data;
- Law No. 26/2018 of 22 October 2018 regarding Electronic Communications in Gabon;
- Law No. 02/2004 of 30 March 2005 ratifying the International Convention for the Suppression of the Financing of Terrorism;
- Regulation No. 01/CEMAC/UMAC/CM of 11 April 2016 on the prevention and suppression of money laundering, terrorist financing and proliferation in Central Africa;
- Law No. 025/2021 of 28/12/2021 regulating electronic transactions in the Gabonese Republic; and
- Law No. 027/2023 of 11/07/2023 regulating cybersecurity and the fight against cybercrime in the Gabonese Republic.

DEFINITIONS

Definition of Personal Data

Any information relating to an identified or identifiable natural person, directly or indirectly, by reference to an identification number or to one or more elements, specific to his physical, physiological, genetic, psychological, cultural, social or economic identity (Article 6 of the Law).

Definition of Sensitive Personal Data

All personal data relating to religious, philosophical, political or trade union opinions or activities, sex life, health, social race, health, social measures, prosecution, criminal or administrative sanctions (Article 6 of the Law).

NATIONAL DATA PROTECTION AUTHORITY

The Gabonese National Authority for Data Protection is The Authority for the Protection of Personal Data and Privacy (known by its French acronym APDPVP).

According to article 8 of the 2023 law on personal data, the main tasks of the APDPVP are to inform the persons concerned and the data controllers of their rights and obligations in terms of personal data. It is also responsible for monitoring the implementation of personal data processing and the protection of privacy.

The APDPVP's remit includes in particular:

- Authorising the processing operations specified in article 80, giving an opinion on those mentioned in articles 81 and 82, and receiving declarations concerning other processing operations.
- Drawing up and publishing standards and issuing model regulations to guarantee the security of systems.

- To receive claims, petitions and complaints relating to the implementation of personal data processing, informing the authors of the action taken.
- Responding to requests for advice from public authorities and the courts, while advising individuals and organisations involved in automated data processing _ personal data.
- To inform the Public Prosecutor of offences found to have been committed and to submit observations relating to criminal law.
- Sessions of chargeur members or agents to carry out checks on personal data processing and, if necessary, obtain copies of relevant documents.
- Pronounce measures and sanctions against a controller in accordance with Articles 199 to 204.
- Respond to requests for access from data subjects to the processing of their personal data.
- To issue opinions on the compliance of draft professional rules, products and procedures for the protection of personal data with the law in force.
- Issue opinions on the guarantees offered by professional rules previously recognised as complying with the law, taking into account the fundamental rights of individuals.
- To issue labels to products or procedures that comply with the law after evaluation.
- Issue opinions on draft laws or decrees relating to the protection of individuals with regard to automated processing.
- Propose legislative or regulatory measures to adapt the protection of freedoms to developments in computer processes and techniques.
- To provide assistance in matters of personal data protection at the request of other bodies and administrations.
- To participate, at the request of the Government, in the preparation and definition of the Gabonese position in international negotiations relating to the protection of personal data and privacy.
- Being part of the Gabonese delegation to the work of the competent Community and international organisations in the field of the protection of personal data and privacy, at the request of the Government.

REGISTRATION

The is no country-wide system of registration in Gabon. However, the processing of personal data may be subject to prior notification to, or authorisation from APDPVP.

The requirement of prior authorisation is applicable in the following circumstances:

- automatic or non-automatic processing of data regarding criminal convictions and infractions, except for processing carried out by Justice officials in the context of their obligations to ensure the security of possibly affected persons;
- automatic processing of genetic data (except when carried out by healthcare professionals for the purpose of preventive medicine, medical diagnosis or the provision of medical care and treatment);
- automatic processing which, considering the nature of the data or of the underlying purpose of processing, may result in excluding an individual from rights, benefits, contributions, or contract(s), without a legal or regulatory basis;
- automatic processing aimed at interconnection by one or more entities in the context of public service aimed at different public interests, or interconnection between different entities, for different purposes;
- processing which concerns a person's registration number in a national identification database;
- automatic processing of data containing comments, observations, and analysis of social difficulties experienced by individuals; and
- automatic processing of biometric data required for controlling the identity of individuals.

The APDPVP shall take a decision within two months from receiving the request for authorisation. This time limit may be renewed once by a decision from the President of the APDPVP. Where theAPDPVP has not taken a decision within these time limits, the application for authorisation shall be deemed to be rejected.

Specific activities for data processing are subject to ministerial approval. These include data processing carried out on behalf of the State and aimed at State security, defence or public safety, or which is carried out for the purpose of preventing, investigating, detecting, pursuing, or executing criminal infractions is approved by the competent Government ministry(ies), subject to a prior opinion by the APDPVP. Other matters are also approved by legislative measures, such as publicly relevant processing aimed at public census.

Other data processing operations are subject to a mere prior notification to the,APDPVP except if a complete exemption from notification or authorisation applies. Specifically, the following activities are exempt from formalities in accordance with article 89 of the aforementioned law:

- processing operations aimed solely at forming a register which is legally intended exclusively for public information and is open to public consultation by any person with legitimate interest;
- processing operations by any organisation, not-for-profit organisation, or any religious, political, philosophical, or trade union organisation or association – this exemption only applies if:
    - the processing operations corresponds to the formal and official purpose of said organisation / association;
    - the processing relates only to its members, and, where applicable, to people who have regular contact with the organisation / association in the context of its activity; and
    - the data is not disclosed to third parties, unless the data subject has given its / her consent;
- processing operations for which the data controller has appointed a data protection officer ('DPO'), unless personal data is being transferred across borders.

In addition, the APDPVP may identify specific data processing operations which, due to their simplicity and low-risk level, may be subject only to a simplified notification process. This simplified process includes:

- the purposes of the processing operations;
- personal data or categories of personal data processed;
- the category or categories of persons concerned;
- the addressees or categories of addressees to whom personal data are communicated; and
- the data retention periods.

DATA PROTECTION OFFICERS

Under the new law on personal data, the appointment of a Data Protection Officer (**DPO**) is no longer left exclusively to the discretion of the data controller. The law establishes the conditions under which a DPO must be appointed and limits the discretionary power of the data controller. These conditions include:

- Where the processing is carried out by a public authority or public body, with the exception of courts acting in the exercise of their judicial function;
- Where the basic activities of the controller or processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic large-scale monitoring of the data subjects;
- Where the basic activities of the controller or processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic large-scale monitoring of the data subjects;
- Where the basic activities of the controller or processor consist of large-scale processing of sensitive data and data relating to convictions for criminal offences.

In addition, a DPO position must be held by a person with the qualifications required to carry out his or her duties, namely professional qualities, particularly relating to knowledge of the law and matters relating to data protection.

The DPO is responsible for ensuring that data processing is compliant. His / her duties cover all processing carried out by the body that appointed him. In this capacity, he / she is responsible for:

- informing and advising the data controller or data processor, as well as the people in the organisation who process the data, of their obligations under this law;
- monitoring compliance with this law and with the internal rules put in place by the data controller or data processor with regard to data protection, including the allocation of responsibilities and the awareness and training of staff involved in data processing and auditing operations;
- giving an opinion on data protection impact assessments and checking that they have been carried out;

to cooperate with the APDPVP, including in the event of prior consultation by the controller when a data protection impact assessment is carried out, and to consult, as appropriate, on any other matter.

COLLECTION & PROCESSING

The data processor must present sufficient guarantees to ensure the security and confidentiality of personal data. This requirement does not relieve the data controller of its obligation to ensure compliance with the measure concerning security and confidentiality displayed in Articles 113 *et seq*. of the Personal Data Act 2023.

The obligations of data controllers include:

- **Transparency**: The data controller must inform the data subject of the terms of processing when the data is not collected from the data subject. In addition, the data controller must inform the data subject at least before the first communication and must also guarantee a lawful basis to carry out the processing operation;
- **Confidentiality**: The data controller must assure that the processing of personal data is only carried out under his authority and instructions. In addition, the data controller must guarantee that only individuals who have technical and legal knowledge regarding the integrity of data, and in this sense the data controller must ensure that the individuals dealing with personal data has signed a non-disclosure agreement;
- **Security**: The data controller is required to take any appropriate precautionary measures in regard to the nature of personal data, and, in particular, the data controller shall prevent personal data from being distorted, damaged, or unauthorised access by third parties. In particular, the data controller must:
    - create different levels of access permissions, on a need-to-know basis depending on the position of its employees, thus avoiding unauthorised actions;
    - use encryption or pseudonymisation;
    - keep a record of who accesses the personal data, when and why, ensuring traceability of its use;
    - maintain backups in secondary sources to prevent accidental changes or loss of data; and
    - ensure the identity of the person who wants to access the data or the identity of the parties to whom the data will be disclosed.
- **Retention**: The data controller must guarantee that the data is kept for no longer than the purpose for which was collected.

The Data Protection Law expressly provides for limited data controller rights, and in practice provides data controllers with the right to:

- process personal data in the conditions provided for by law;
- refuse compliance with unreasonable requests and demands from data subjects; and
- appeal any sanctioning decisions by the APDPVP before the State Counsel.

By contrast, the data subject are entitled to the following rights provided for in Articles 52 and 53 of the aforementioned Personal Data Act 2023:

- obtain all of their personal data in an understandable form, as well as any available information as to the origin;
- oppose, for legitimate reasons, the processing of personal data concerning them;
- oppose the processing of their personal data for prospecting purposes;
- rectify, complete, update, lock, or delete personal data concerning them, where it is inaccurate, incomplete, equivocal, out of date, or if collection, use, communication or conservation is prohibited; and
- not be subject to decisions made on the sole basis of an automated processing that would produce significant or detrimental legal repercussions for them.

Interconnection of personal data shall:

- not discriminate against or infringe on the fundamental rights, freedoms, and guarantees of holders of the data;
- ensure the use of appropriate safety measures; and
- take into account the principle of relevance (Article 169 of the Personal Data Act 2023).

TRANSFER

Data transfers to another country are prohibited unless the other country ensures an adequate level of privacy protection and protection of fundamental rights and freedoms of individuals with regard to the processing operation.

The list of countries that comply with this adequate level of protection shall be published by APDPVP (article 171 in fine of the law on personal data). As far as we are aware, this list has not yet been published. However, the Data Protection Law of 2023 in its article 171 does identify the criteria which must be considered by the APDPVP in order to determine adequacy:

- the legal provisions existing in the country in question;
- the security measures enforced;
- the specific circumstances of the processing (such as the purpose and duration thereof); and
- the nature, origin, and destination of the data.

As an alternative to the 'adequacy' criteria, Article 76 of the aforementioned law allows those data controllers to transfer data if:

- the data subject has consented expressly to its transfer;
- the transfer is necessary to save that person's life;
- the transfer is necessary to safeguard a public interest;
- the transfer is necessary to ensure the right of defence in a court of law; or
- the transfer is necessary for the performance of a contract between the data subject and the data controller, at the request of the data subject, or for the performance of a contract between the data controller and a third party in the interest of the data subject.

Please kindly note that, except in very specific circumstances, the international transfer of non-encrypted personal data for the purpose of investigation in the health sector is not possible, given the sensitivity of the data at stake.

In relation to outsourcing, the Data Protection Law of 2023 does not provide for specific provisions, except:

- the obligations applicable to the relationship with data processors;
- when data processors are located outside the country, the provisions applicable to international data transfers; and
- general security obligations, which vary depending on the nature of the data at stake (Articles 168 *et seq.* of the aforementioned law).

No references are included to specific concerns regarding, for example, outsourcing to the cloud or to data centres.

SECURITY

Articles 113 et seq. of the 2023 Personal Data Act state that in order to guarantee the security of personal data, the data controller is required to take all necessary precautions with regard to the nature of the data and, in particular, to prevent it from being distorted, damaged or accessed by unauthorized third parties. In particular, he / she shall take all measures to:

- guarantee that, for the use of an automated data processing system, authorized persons can only access personal data within their competence;
- guarantee that the identity of third parties to whom personal data may be transmitted can be verified and established;
- guarantee that the identity of persons who have had access to the information system and which data have been read or introduced into the system, at what time and by which person, can be verified and established posteriori;
- prevent any unauthorized person from accessing the premises and equipment used for data processing;
- prevent data carriers from being read, copied, modified, destroyed or moved by an unauthorized person;
- prevent the unauthorized entry of any data into the information system and the unauthorized access, modification or deletion of stored data;
- prevent the use of data processing systems by unauthorized persons using data transmission facilities;
- prevent unauthorized reading, copying, modification or deletion of data during data communication and transport of data carriers;
- back up data by making back-up copies;
- Refresh and, if necessary, convert the data for permanent storage.

No specific requirements other than those set forth in the Law.

BREACH NOTIFICATION

There is a legal requirement to notify data breaches to APDPVP. For more details please refer to "Mandatory Breach Notification" below.

Mandatory breach notification

Under article 142 of the Data Protection Act, in the event of a data breach, the data controller is required to notify the Personal Data Protection and Privacy Authority (APDPVP) without delay. This notification must include the nature of the breach, the categories and approximate number of persons concerned, the measures taken or envisaged to remedy the breach, and the contact details of the Data Protection Officer or another contact point for further information.

In addition, if the breach is likely to result in a high risk to the rights and freedoms of the data subjects, the data controller must inform the data subject individually as soon as possible, as specified in article 145 of the aforementioned law. This communication must be made in clear and simple terms, describing the nature of the breach and providing the information and measures necessary to remedy the situation, in accordance with article 146 of the aforementioned law.

However, there are specific cases where communication to the data subject is not necessary, as provided for in Article 147 of the aforementioned Data Protection Act. These cases include, in particular, where the data controller has taken measures to protect the data affected by the breach, has taken preventive measures against any high risk to the rights and freedoms of the data subjects, or finds that communication would require disproportionate efforts. In such cases, the controller must make a public announcement or take a similar measure enabling the data subjects to be informed in an equally effective manner.

ENFORCEMENT

The law empowers the APDPVP to impose various sanctions depending on the severity of the infringement. However, the level of enforcement remains quite low due to resource limitations and the fact that this field of law is still new to the administration and business and data subjects.

In fulfilment of their duties, members of the APDPVP and sworn and authorized officials have access to places, premises, enclosures, installations or establishments used for the processing of personal data and which are for professional use, with the exception of those parts of the premises used for private purposes.

They are accompanied by Officers of the Judicial Police during inspection missions. The Public Prosecutor responsible for the area is informed in advance.

If the person in charge of the premises objects, the visit may only take place with the authorization of the President of the court in whose jurisdiction the premises to be visited are located or the judge delegated by him.

The Authority shall assess and impose the following measures or penalties, without graduation, depending on the breach of this law found:

- a warning to the data controller who fails to comply with the obligations arising from this law;
- a formal notice to cease the breaches observed within a period set by the Authority;
- a financial penalty.

The APDPVP may impose the following sanctions:

- temporary suspension from collecting and processing personal data for a period of three months, at the end of which the suspension becomes definitive;
- a fine of between one million and one hundred million CFA francs.

The amount of the fine shall be proportionate to the seriousness of the breaches committed and the benefits derived from the breach.

For the first breach, it may not exceed XOF ninety-eight million four hundred thousand. In the event of a repeat offence, it may not exceed XOF three hundred million or, in the case of a company, 5% of turnover excluding tax for the last financial year for which the accounts have been closed, subject to a limit of XOF one hundred and ninety-six million.

Where the APDPVP has imposed a financial penalty that has become final before the criminal court has given a final ruling on the same or related facts, the criminal court may order that the financial penalty be deducted from the fine it imposes.

Penalties are recovered in accordance with the legislation relating to the recovery of State tax debts.

Additional administrative penalties may also apply.

Moreover, criminal offences resulting from violation of the provisions of this law are punishable in accordance with the provisions of the Criminal Code.

Obstructing the work of the APDPVP is punishable by a prison sentence of between six months and one year and a fine of between XOF one million and XOF ten million, either by:

- opposing the performance of the tasks entrusted to its members or authorised agents;
- refusing to provide its members or authorised agents with information and documents useful for their work, or by concealing said documents or information, or by making them disappear;
- communicating information that does not correspond to the content of the recordings as it was at the time the request was made or that does not present this content in a directly accessible form.

In the event of a repeat offence, the penalties provided for in the law shall be doubled.

ELECTRONIC MARKETING

The personal data Act will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name).

The general rule for electronic marketing is that it requires the express consent of the recipient (see Article 37 of Law No. 025 /2021 of 28/12/2021 regulating electronic transactions in the Gabonese Republic).

Even when a marketer has the consent of a data subject, that consent can be withdrawn by the data subject under Article73of the Personal Data Act.

The data subject has the right to object at any time to the use of his / her personal data for such marketing under Article 60 of the Personal Data Act.

This right to object must be explicitly brought to the attention of the data controller.

However, in accordance with article 60 of the aforementioned law, the data controller may not respond favorably to a request to exercise the right to object if it demonstrates the existence of legitimate reasons justifying the processing, which override the interests, fundamental rights and freedoms of the data subject.

ONLINE PRIVACY

The Law does not provide any specific rules for governing cookies and location data.

However, pursuant to Article 113 and sq. of the data law mentioned above, data controller must implement all appropriate technical and organizational measures to preserve the security and confidentiality of the data, including protecting the data against accidental or unlawful destruction, accidental loss, alteration, distribution or access by unauthorized persons.

KEY CONTACTS

Geni & Kebe

www.dlapiperafrica.com/senegal

Dr. Sangare Mouhamoud
Associate
Geni & Kebe
T +225077910754l
m.sangare@gsklaw.sn

Dr. Francky Lukanda
Senior Associate
Geni & Kebe
T +2250584344660
f.lukanda@gsklaw.sn

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

GEORGIA

Last modified 22 December 2021

LAW

The Law of Georgia On Personal Data Protection (N5669-RS, 28/12/2011) (‘**PDP Law**’).

DEFINITIONS

Definition of Personal Data

Personal data: any information connected to an identified or identifiable natural person. A person is identifiable when he/she may be identified directly or indirectly, in particular by an identification number or by any physical, physiological, psychological, economic, cultural, or social features specific to this person.

Definition of Sensitive Personal Data

Special category data: data connected to a person's racial or ethnic origin, political views, religious or philosophical beliefs, membership of professional organisations, state of health, sexual life, criminal history, administrative detention, putting a person under restraint, plea bargains, abatement, recognition as a victim of crime or as a person affected, also biometric and genetic data that allow to identify a natural person by the above features.

Biometric data: Any physical, mental, or behavioural feature which is unique and constant for each natural person and which can be used to identify this person (fingerprints, footprints, iris, retina (retinal image), facial features).

Genetic data: Unique and constant data of a data subject relating to genetic inheritance and/or DNA code that makes it possible to identify them.

NATIONAL DATA PROTECTION AUTHORITY

State Inspector Service (‘State Inspector’).
www.personaldata.ge

REGISTRATION

With certain exceptions (discussed below), there is no requirement under PDP Law to notify or register before processing personal data.

The registration requirement applies to the databases. According to the PDP Law, a database is any structured set of personal data where data is arranged and can be accessed based on certain criteria. The PDP Law uses the term filing system to denote a database. For example, a customer database or a registry of employees and clients that is subject to processing may qualify as a filing system.

The data controller is obliged to have a catalogue on each filing system that provides a detailed description of the filing system's structure and content.

According to the PDP Law, before creating a filing system and entering in any new category of data, a data controller shall notify the State Inspector and register the following information about the filing system:

- The name;
- The names and addresses of a data controller and a data processor;
- The place of storing or processing of data;
- The legal grounds for data processing;
- The category or categories of data subjects;
- The data category or categories in a filing system;
- The purpose of data processing;
- The period of data storage;
- The facts and grounds for restriction (if any) of any data subject rights;
- The recipient of data stored in a filing system, and their categories;
- Information on any cross-border data transfer and transmission of data to international organisation and the legal grounds for the transfer;
- A general description of the procedure established to ensure data safety.

The data controller shall regularly update the filing system catalogue and notify the Inspector about any alteration made to the information, no later than 30 days after the alteration.

The notification requirement also applies to cross-border data transfer and a private organisation's processing of a biometric data.

Before using the biometric data, a data controller must provide the State Inspector with the same information that is provided to the data subject, specifically the purpose of data processing and the security measures taken to protect the data.

DATA PROTECTION OFFICERS

None.

COLLECTION & PROCESSING

The following minimum requirements must be met when collecting or otherwise processing the personal data:

- A proper legal ground (for example, a data subject's consent) exists to process the data;
- The personal data is processed for specific, clearly defined, and legitimate purposes;
- The personal data is processed only to the extent necessary for legitimate purposes;
- The personal data is adequate and proportionate to the purpose or purposes for which it was collected and processed;
- The data is kept only for the period necessary to achieve the processing's purpose;
- The data controller or data processor takes technical and organisational security measures to ensure the protection of personal data against accidental or illegal destruction, modification, disclosure, access, and any other form of illegal use or accidental or illegal loss;
- The security measures implemented are appropriate to the risks related to the data processing.

TRANSFER

Transfer of personal data outside Georgia is admissible without a separate authorisation from the State Inspector if one of the two following conditions apply:

- A respective legal ground for data processing exists and the proper standards for the safety of data are secured in the relevant country. The State Inspector has approved the list of such countries;
- The processing of data is stipulated under an international agreement between Georgia and the relevant country;

However, the general data processing rules will still apply, including securing a necessary legal ground such as the data subject's consent and the requirements of proportionality and necessity.

If neither of these conditions apply, then there should be a formal written agreement between the transferor and the data's recipient under which the data's recipient shall commit to ensure proper guarantees to protect the data. In this case, the State Inspector must be presented with such agreement and other relevant information or documents for data transfer approval.

SECURITY

A data processor must implement technical and organisational security measures to ensure the protection of personal data against accidental or illegal destruction, modification, disclosure, access, and any other form of illegal use or accidental or illegal loss. The security measures implemented must be appropriate to the risks related to the data processing.

A record must be kept of all data processing activities carried out on personal data stored in electronic form. A record must also be kept of any disclosure or modification of personal data contained in non-electronic form.

Employees of a data controller or a data processor who are involved in data processing must not act beyond the scope of the powers conferred upon them. Employees must be bound to protect confidentiality of the personal data, including after termination of their official duties.

BREACH NOTIFICATION

None.

ENFORCEMENT

The State Inspector has power to carry out inspections of any data controller and data processor on its own initiative or based on complaints received from data subjects.

The State Inspector may order:

- Temporary or permanent termination of data processing;
- The blocking, destruction, or depersonalisation of personal data;
- The termination of transfer;
- An issuance of administrative fines.

The State Inspector also has a duty to report any violations of a criminal nature to the competent authority. The liability for violation of the data privacy can be criminal, administrative or civil.

Criminal liability: a fine, correction labour, imprisonment for three years, or all three may result from illegal collection, retention, use, or dissemination of personal data that caused substantial damage; A legal entity may be imposed a fine, deprivation of the right to run the business, liquidation and a fine for the same action.

Administrative sanctions: ranging from GEL500 (app. USD 160) to GEL10,000 (app. USD 3200) depending on the type of violation.

Civil: claims can be brought by individuals, depending on the damage the breach of the PDP Law caused.

ELECTRONIC MARKETING

PDP Law defines direct marketing as offering of goods, services, employment, or temporary work by mail, telephone calls, email, or any other telecommunication facility.

Consent is not required to process personal data obtained from public sources for direct marketing purposes. The data permissible to be collected from publicly available sources is limited to: name and surname, telephone number, email, and fax number.

However, written consent is required if the data processor wishes to use other types of personal data for direct marketing purposes.

Individuals are entitled to demand the termination of using their data for direct marketing purposes at any time in the form under which the direct marketing is conducted.

ONLINE PRIVACY

There is no special regulation with respect to cookies and general rules on data collection and processing applies. Georgian websites routinely ask for cookie consent.

There is no requirement to store data in Georgia. However, rules on cross border data transfer will apply.

KEY CONTACTS

MKD Law
mkdlaw.ge/en

Baqar Palavandishvili
Lawyer
MKD Law
T +995 32 2553880/81
bpalavandishvili@mkdlaw.ge

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

GERMANY

Last modified 19 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

Germany has adjusted the German legal framework to the GDPR by passing the new German Federal Data Protection Act (*Bundesdatenschutzgesetz* – "**BDSG**"). The BDSG came into force together with the GDPR on May 25, 2018. The purpose of the BDSG is especially to make use of the numerous opening clauses under the GDPR which enable Member States to specify or even restrict the data processing requirements under the GDPR. Part 3 of the BDSG implements the Law Enforcement Directive (EU) 2016/680.

Find the English version here.

In addition to the BDSG, there exist a number of data protection rules in area-specific laws, for example those regulating financial trade or the energy sector. As of 1 December 2021, the Telecommunications-Telemedia-Data Protection Act (*Telekommunikation-Telemedien-Datenschutzgesetz* – "**TTDSG**") provides data protection regulations for telecommunication and telemedia providers, which are intended to eliminate a long-standing legal uncertainty about the applicability of the data protection regulations of the German Telecommunications Act (*Telekommunikationsgesetz* – "**TKG**") and the German Telemedia Act (*Telemediengesetz* – "**TMG**") in interaction with the GDPR. The TTDSG also transposes the “cookie consent” requirement under Article 5 (3) ePrivacy Directive into German law.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions are the same as in Article 4 GDPR. Beyond that, the BDSG contains further definitions for 'public bodies of the Federation', 'public bodies of the Länder' and 'private bodies' in Section 2 BDSG. The TTDSG contains definitions for types of data that are specifically related to the provision of telecommunications and telemedia services (so-called inventory data and usage data).

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the CNIL in France or the Garante in Italy). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Germany does not have one central supervisory authority for data protection law but authorities in each of the sixteen German federal states (*Länder*) that are competent for the public and the private sector in the respective state. In

addition, there are different supervisory authorities for private broadcasters as well as for public broadcasters and several supervisory authorities for religious communities.

The German Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für Datenschutz und Informationsfreiheit* – "**BfDI**") is the supervisory authority for all federal public bodies as well as for certain social security institutions; it also supervises telecommunications and postal service providers, insofar as they provide telecommunications or postal services. The BfDI represents Germany in the European Data Protection Board. To ensure that all the supervisory authorities have the same approach, a committee consisting of members of all authorities for the public and the private sector has been established – the 'Data Protection Conference' (*Datenschutzkonferenz* "**DSK**"). The coordination mechanism between the German supervisory authorities for data protection law mirrors the consistency mechanism under the GDPR.

A list with the contact details and websites of most of the supervisory authorities can be found here.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

There is no general requirement in Germany for controllers or processors to register their processing activities with the competent supervisory authority for data protection law; however, a register of data protection officers (DPOs) is maintained.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer (DPO) if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single DPO with responsibility for multiple legal entities (Article 37(2)), provided that the DPO is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single DPO).

DPOs must have "expert knowledge" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The threshold to designate a DPO is much lower in the BDSG. The controller and processor has to designate a DPO if they constantly employ as a rule at least 20 persons dealing with the processing of personal data by automated means, Section 38 (1) sentence 1 BDSG. The meaning of ‘automated processing’ is interpreted broadly by the German Authorities. It basically covers every employee who works with a computer.

If the threshold of 20 persons is not reached, Section 38 (1) sentence 2 BDSG regulates, that a DPO has to be designated in case the controller or processor undertakes processing subject to a data protection impact assessment pursuant to Article 35 GDPR, or if they commercially process personal data for the purpose of transfer, of anonymized transfer or for purposes of market or opinion research.

A dismissal protection for the DPO is provided in Section 38 (2) in conjunction with Section 6 (4) BDSG. Where the controller or processor is obliged to appoint a DPO, the dismissal of a DPO, who is an employee, is only permitted in case there are facts which give the employing entity just cause to terminate without notice. After the activity as DPO has ended, a mandatory DPO who is an employee may not be terminated for a year following the end of appointment, unless the employing entity has just cause to terminate without notice.

Additionally, Section 38 (2) in conjunction with Section 6 (5) and (6) BDSG stipulates that the DPO shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified, unless he / she is released from this obligation by the data subject. Also, the DPO has the right to refuse to give evidence under certain conditions.

Moreover, the German supervisory authorities expect that the DPO speaks the language of the competent authority and the data subjects, i.e. German, or at least that instant translation is ensured.

The supervisory authorities maintain a register of DPOs. No fee is charged for registering or updating the details of a DPO.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known as lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;

- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;

- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when the European Union’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The BDSG has additional rules regarding processing of special categories of personal data. Contrary to Article 9 (1) GDPR, processing of such data is permitted by public and private bodies in some cases which are based on the exceptions in Article 9 (2) GDPR, see Section 22 (1), 26 (3) BDSG. Also, Section 24 BDSG determines cases in which controllers are permitted to process data for a purpose other than the one for which the data were collected.

Section 4 BDSG provides a special rule for video surveillance of publicly accessible areas. According to the German data protection supervisory authorities as well as the German Federal Administrative Court (*Bundesverwaltungsgericht* – "**BVerwG**") and the near unanimous opinion in German legal literature, the provision is not compliant with the GDPR insofar as it regulates surveillance by private bodies (Section 4 (1) Nos. 2, 3 BDSG). This is based on the argument that the GDPR does not contain any opening clause on which these deviations from Article 6 (1) GDPR could be based.

Furthermore, the BDSG provides special rules regarding processing for employment-related purposes in Section 26 BDSG. The German legislator has made very broad use of the opening clause in Article 88 (1) GDPR and has basically established a specific employee data protection regime, that mostly only repeats the general legal bases of performance of contract respectively “*carrying out the obligations and exercising specific rights… in the field of employment and social security and social protection law*” (Art. 9(2)(b) GDPR). Due to this, the European Court of Justice ruled that a provision in German state data protection law (which applies to the public sector) that corresponds with the “ performance of the employment contract” legal basis in Section 26 BDSG is invalid (Judgment of the CJEU in Case C-34/21). This is because the law failed to establish specific provisions, although this is a requirement pursuant Article 88 (1) GDPR for national legal bases. Due to this decision, it is widely assumed (including by the German supervisory authorities that (some) of the respective German legal bases for the processing of employee personal data in the BDSG are invalid.

Employers should therefore rely (alternatively or additionally) on the GDPR legal bases for the processing of employee and candidate personal data for the establishment or the performance of the employment contract (Article 6(1)(b) GDPR) respectively on Article 9(2)(b) GDPR. In particular when determining what is “necessary” for the performance of the employment contract, employers also need to comply with the case law of the German Federal Labour Court (*Bundesarbeitsgericht* – "**BAG**").

In addition, there is a legal basis specifically for the investigation of criminal offences against employees which likely is still valid.

Furthermore, processing of employee personal data for purposes that are not specifically related to employment as such can still be based on Article 6 (1) GDPR. In particular, controllers that are part of a group of companies may be able to base transfers of data within the group for internal administrative purposes on their legitimate interests in accordance with to Article 6 (1) f) (as stated by Recital 48 of the GDPR).

The processing of personal data in the context of the provision of telecommunication services is subject to Section 9 et seqq. TTDSG. Furthermore, both the content of telecommunications and its detailed circumstances, in particular the fact whether someone is or was involved in a telecommunications process, is subject to the secrecy of telecommunications, Section 3 TTDSG. Violations of the secrecy of telecommunications constitutes a criminal offence under the German Criminal Code (*Strafgesetzbuch* – "**StGB**").

The processing of personal data in the context of the provision of telemedia (like for example a website or a social network) is subject to specific limitations contained in Section 19 et seqq. TTDSG. There are, inter alia, specific requirements regarding the provision of inventory data, passwords or usage data to public authorities in Section 22 et seqq. TTDSG.

The following German specific rules for the processing of personal data in the employment context likely are still valid:

- Employees’ personal data may be processed to detect criminal offenses only if there is a documented reason to believe the data subject has committed such an offense while employed, the processing of such data is necessary to investigate the offense and is not outweighed by the data subject’s legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason (Section 26 (1) sentence 2 BDSG) (this blocks investigation based on legitimate interests pursuant Article 6(1) f GDPR);
- The processing is based on a works council agreement which complies with the requirements set out Article 88 (2) GDPR (Section 26 (4) BDSG);
- The processing is based on the employee’s consent in written or electronic form. A derogation from this form can apply if a different form is appropriate because of special circumstances (but this derogation will rarely apply in practice). Moreover, the utilization of consent as basis for the processing is particularly problematic in Germany as Section 26 (2) BDSG stipulates requirements in addition to Article 7 GDPR. If personal data of employees are processed on the basis of consent, then the employee’s level of dependence in the employment relationship and the circumstances under which consent was given shall be taken into account in assessing whether such consent was freely given. Consent may be freely given in particular if it is associated with a legal or economic advantage for the employee, or if the employer and employee are pursuing the same interests. The German data protection supervisory authorities interpret this provision in a way that employee consent cannot be used for processing of personal data which directly relates to the employment relationship, but only to supplementary services offered by the employer (e.g. private use of company cars or IT equipment, occupational health management or birthday lists).

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on the condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or

g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The transfer of personal data to a third country or to supranational or intergovernmental bodies or international organisations in the context of activities not falling within the scope of the GDPR or the Law Enforcement Directive (EU) 2016/680 are also permitted if they are necessary for the performance of own tasks for imperative reasons of defence or for the performance of supranational or intergovernmental obligations of a federal public body in the field of crisis management or conflict prevention or for humanitarian measures.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However, the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The BDSG has additional rules regarding the processing of special categories of personal data in Sec. 22 (2) BDSG. In case of processing of such data, appropriate and specific measures have to be taken to safeguard the interests of the data subject.

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, these measures may include in particular the following:

- technical and organizational measures to ensure that processing complies with the GDPR;

- measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed;
- measures to increase awareness of staff involved in processing operations;
- designation of a data protection officer;
- restrictions on access to personal data within the controller and by processors;
- the pseudonymization of personal data;
- the encryption of personal data;
- measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;
- specific rules of procedure to ensure compliance with this Act and with the GDPR in the event of transfer or processing for other purposes.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

Personal data breaches should be notified to the competent supervisory authority. The German supervisory authorities generally make available specific web forms for notifications and some of them have published risk rating requirements for personal data breach notifications.

The German BDSG only contains slight changes and additions to the regulations in Article 33, 34 GDPR.

Section 29 (1) BDSG stipulates in addition to the exception in Article 34 (3) GDPR, the obligation to inform the data subject of a personal data breach according to Article 34 GDPR shall not apply as far as meeting this obligation would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party. By derogation from this, the data subject pursuant to Article 34 GDPR shall be informed if the interests of the data subject outweigh the interest in secrecy, in particular taking into account the threat of damage.

According to Section 43 (4) BDSG, a notification pursuant to Article 33 GDPR or a communication pursuant to Article 34 (1) GDPR may be used in proceedings pursuant to the Act on Regulatory Offences (*Gesetz über Ordnungswidrigkeiten* – "**OWiG**") against the person required to provide a notification or a communication only with the consent of the person obligated to provide a notification or a communication.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

In October 2019 the German data protection authorities published guidelines for calculating administrative fines against ‘business undertakings’ under Article 83 GDPR. However, since the final version of the Guidelines 04 /2022 on the calculation of administrative fines under the GDPR of the EDPB was adopted in May 2023, the German guidelines are no longer relevant.

Enforcement powers

There are no German specific enforcement powers except for the German Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für Datenschutz und Informationsfreiheit* – "**BfDI**") competent for federal authorities and certain sectors (see Authority for details).

Administrative powers

German law provides for administrative fines of up to 50,000 EUR for the violation of German specific requirements for the processing of personal data in the context of consumer loans (Sections 30 and 43 BDSG).

Criminal offences

The BDSG provides for several offences which can result in prosecution of, imprisonment, and criminal penalties being imposed of / on individuals. The offences under the BDSG include:

- transferring personal data to a third party or otherwise making them accessible if done deliberately and without authorization for commercial purposes and with regard to the personal data of a large number of people which are not publicly accessible;
- processing without authorization, or fraudulently acquiring, personal data which are not publicly accessible if doing so in return for payment or with the intention of enriching oneself or someone else or harming someone.

Additionally other special laws provide for criminal offences (e.g. violations of the secrecy of telecommunications constitutes a criminal offence under the German Criminal Code (*Strafgesetzbuch* – StGB)).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon,

the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is likely to be replaced by a regulation (the so called ePrivacy Regulation), but it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

In general, unsolicited electronic marketing requires prior opt-in consent. The opt-in requirement is waived under the ‘ same service / product’ exemption. The exemption concerns marketing emails related to the same products/services as previously purchased from the sender by the user provided that:

- the user has been informed of the right to opt-out prior to the first marketing email
- the user did not opt-out, and
- the user is informed of the right to opt-out of any marketing email received. The exemption applies to electronic communication such as electronic text messages and email but does not apply with respect to communications sent by fax.

Direct marketing emails must not disguise or conceal the identity of the sender.

Like the GDPR, the German BDSG also does not provide for any specific provisions regarding marketing. The use of electronic communication for the purpose of direct marketing as currently regulated in ePrivacy Directive has been transposed into German law and is implemented in Section 7 of the German Act Against Unfair Competition (*Gesetz gegen den unlauteren Wettbewerb* – "**UWG**") As emphasized by the German Authorities (in their guidelines on direct marketing), processing of personal data for the purpose of marketing communication which is in breach of Section 7 UWG also constitutes a breach of the GDPR as it does not follow a legitimate purpose.

When using electronic communication for direct marketing, prior consent is generally required, cf. Section 7 (2) no. 1, 2 UWG, the standard for this being the so-called double opt-in process. According to Article 6 (1) a) GDPR as well as according to established German case law, data subjects must always give consent for a specific processing purpose. This means that the person to be contacted needs to know (1) from whom (meaning which specific entity or entities), (2) for which specific products and services he / she will receive marketing offers and (3) by which means (e.g. email or telephone).

The German lawmaker has also transposed the ‘same service / product’ exemption into Section 7 UWG. Based on Section 7 (3) UWG, direct marketing can be based on the exemption if the following prerequisites are met:

- the recipients electronic mail address was obtained from the sender in connection with the sale of goods or services;
- the sender uses the address for direct advertising of his own similar goods or services (no cross-selling permitted);
- the recipient has not objected to this use; and

- the recipient is clearly and unequivocally advised, upon the collection of the address as well as each time it is used, that he or she can object to such use at any time, without costs arising by virtue thereof, other than transmission costs pursuant to the basic rates.

ONLINE PRIVACY

The General Data Protection Regulation (GDPR) supersedes national data protection law unless there is an opening clause constituted under GDPR. Due to Article 95 GDPR this is the case for national data protection law that was created to implement the Directive on privacy and electronic communication (Directive 2002/58/EC; "ePrivacy Directive").

The German legislator created national data protection regulations for providers of telecommunication services and for providers of certain electronic information and communication services (e.g. website operators) within the TTDSG, which was adopted on 1 December 2021. The TTDSG aims to eliminate the legal uncertainties caused by the fact that special data protection provisions were previously regulated in two different laws, the TKG and the TMG, which were both not adapted to the GDPR. As a result, in the past German data protection authorities and courts sometimes disagreed on which of these provisions, if any, were applicable.

The TTDSG eliminates some provisions that were deemed unapplicable and shifts the data protection regulations regarding telecommunication and telemedia into a single law, which stands alongside the GDPR and the BDSG. The TKG and the TMG have been amended and remain effective, but no longer contain data protection regulations. Whether this new legislation will actually put an end to the previous discussions remains to be seen.

Cookie compliance

The legal requirements with regard to the use of cookies were long unclear in Germany. It was disputed whether there was any consent requirement for cookies at all, as the respective provisions of the ePrivacy Directive had never been transposed into German law (which was also the opinion of the German data protection authorities at that time). Cookie consent was then required as of 28 May 2020, when the German Federal Court of Justice (*Bundesgerichtshof* – "**BGH**") ruled that Section 15 (3) TMG (which technically only provides for an opt-out requirement regarding the use of cookies) was to be construed as a requirement for cookie consent in the meaning of the ePrivacy Directive.

With Section 25 TTDSG, Germany finally transposed Article 5 (3) of the ePrivacy Directice into national law in December 2021, making cookie consent a legal obligation while explicitly including the definition of consent in terms of the GDPR.

In accordance with the ePrivacy Directive, under German law consent is not required where the sole purpose of cookies (or to be more precise, of the storage of information or access to information already stored in the users terminal equipment) is carrying out the transmission of a communication over a public telecommunications network or providing a telemedia service explicitly requested by a user (Section 25 (2) TTDSG).

In addition to that, the German data protection authorities have long been of the opinion that the processing of personal data enabled by the cookies used for analysis and tracking tools regularly requires consent, in particular if the tools allow third parties to collect data from website users as (joint) controllers. It remains to be seen whether this position will be upheld by the BGH or another superior German court.

Traffic data

Lawful processing of traffic data is governed by Section 9 et. seqq. TTDSG and may only take place to the extent it is necessary for the purposes constituted therein or if other legal provisions require a processing. Those who provide or participate in the provision of telecommunication services have to take the technical precautions and actions necessary to protect personal data in accordance with Section 165 TKG; in this context the state of the art must be observed. In addition, the service providers are required to protect the secrecy of telecommunications, which extends to both the content of telecommunications and its detailed circumstances, in particular the fact whether someone is or was involved in a telecommunications process.

Providers of telecommunication services in terms of Section 3 (2) sentence 1 TTDSG may process traffic data for the establishment and maintaining of a telecommunications connection, remuneration inquiry and billing, fraud prevention as well as detection and remedy of disruptions regarding telecommunications systems and tracing of malicious or nuisance calls. Processing of traffic data for marketing purposes, need-based design of telecommunication services and provision of value-added services requires consent in accordance with GDPR.

Generally, traffic data shall be deleted by the service provider without undue delay after termination of each telecommunications connection or as soon as the data are no longer necessary in relation to the purpose for which they are otherwise being processed. However, data may and must be stored in case statutory retention periods under the TTDSG, TKG or other law apply.

If there is a particular and significant risk of a security incident, providers of publicly available telecommunication services shall notify the users about any possible protective or remedial measures that can be taken by users and, where appropriate, about the threat itself (Section 168 (6) TKG), in addition to their general notification obligations with respect to security incidents towards the German Federal Network Agency (*Bundesnetzagentur –* "**BNetzA**") and the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik –* "**BSI**").

Location data

Publicly available telecommunication services may only process location data for the purpose of providing value-added services in case the data are rendered anonymous or processing is based on consent in terms of the GDPR (Section 13 (1) TTDSG).

Consent can be withdrawn at any time and where consent was given to the processing of location data, it must be possible, by simple means and free of charge, to temporarily prohibit the processing of such data for each connection to the network or for each transmission of a message.

The processing of location data in other contexts than telecommunication services (like for example GPS tracking) is subject to the GDPR.

KEY CONTACTS

Verena Grentzenberg
Partner
T +49 40 188 88 203
verena.grentzenberg@dlapiper.com

Dr. Jan Geert Meents
Partner
T +49 89 23 23 72 130
jan.meents@dlapiper.com

Jan Pohle
Partner
T +49 221 277 277 391
jan.pohle@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

GHANA

Last modified 19 January 2024

LAW

The primary legislation governing privacy / data protection in Ghana is the Data Protection Act, 2012 (Act 843).

Other laws, examples of which are set out below, contain some privacy/data protection provisions:

1992 Constitution

Article 18(2) provides citizens with a fundamental right to privacy. The Article provides that *“no person shall be subjected to interference with the privacy of his home, property, correspondence or communication except in accordance with law and as may be necessary in a free and democratic society for public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.”*

Electronic Communications Act, 2008 (Act 775)

A network operator or a service provider who is a holder of a Class Licence shall not use or permit another person to use or disclose confidential, personal or proprietary information of a user, another network operator or service provider without lawful authority unless the use or disclosure is necessary for the operation of the network or service, the billing and collection of charges, the protection of the rights or property of the operator or provider, or the protection of the users or other network operators or service providers from the fraudulent use of the network or service.

A person who intentionally uses or discloses personal information in contravention of the Act commits an offence and is liable on summary conviction to a fine of not more than one thousand five hundred penalty units or to a term of imprisonment of not more than four years or both.

Act 775 defines a Class Licence as *“a licence, other than an individual licence, granted on the same terms to each applicant in respect to a class of electronic communications networks or services or radio-communication services.”*

Electronic Communications Regulations, 2011 (L.I. 1991)

The principle of privacy and secrecy in electronic communications applies to the National Communications Authority, operators of electronic communications networks and providers of electronic communications services.

The operator is required to comply with international best practices in the industry to promote privacy, secrecy and security of communications carried or transmitted by the operator or through the communications system of the operator, and the personal and accounts data related to subscribers.

Credit Reporting Act, 2007 (Act 726)

The Bank of Ghana has the overall supervisory and regulatory authority under the Act to: (a) register, license and regulate bureaus, data providers and credit information recipients and their agents; and (b) control and supervise activities of the credit bureaus, data providers, credit information recipients and their agents.

The Act requires the recipient of a credit report to keep such report confidential while ensuring that the information contained in it is used solely for its specified purpose. A credit bureau, data provider or credit information recipient is required to observe the principles of: (a) equality of credit information subjects; (b) confidentiality of information; (c) non-interference in the private life of citizens; (d) respect for the rights, liberties and lawful interests of persons and legal entities; (e) accuracy and transparency of information; and (f) `privacy and secrecy of communication.

Credit Reporting Regulations, 2020 (L.I. 2394)

These regulations made pursuant to the Credit Reporting Act, 2007 (Act 726), set standards for the safety and security of credit information, standards for data submission by data providers as well as standards for privacy and data security which are to be observed credit bureaus. These include:

- Confidentiality of credit information;
- Controls and security measures to be taken by credit bureaus; and
- Standards to be observed in the processing of data submitted.

*A penalty unit is equivalent to GHS12 (approximately USD11.6 as at 22 December 2023).

Public Health Act, 2012 (Act 851)

Article 45 of the International Health Regulations (2005) of World Health Organisation Regulations which is annexed to Act 851 as the Seventh Schedule provides that *“health information collected or received by a State Party pursuant to these Regulations from another State Party or from WHO which refers to an identified or identifiable person shall be kept confidential and processed anonymously as required by national law.”*

Children’s Act, 1998 (Act 560)

The purpose of this Act is to reform and consolidate the law relating to children, to provide for the rights of the child, maintenance and adoption, regulate child labour and apprenticeship, and provide for ancillary matters concerning children generally.

Act 560 provides that *“a child’s right to privacy must be respected throughout the proceedings at a Family Tribunal”.* In furtherance of this, the Act restricts participants to the sittings of the Family Tribunal to persons with an interest in the matter including parents of the child and officers of the Tribunal.

Act 560 further provides that it is an offence for any person to *“publish any information that may lead to the identification of a child in any matter before a Family Tribunal except with the permission of the Family Tribunal.”*

Cybersecurity Act, 2020 (Act 1038)

The purpose of this Act is to regulate cybersecurity activities in Ghana, promote the development of cybersecurity and to provide for other related matters. This Act permits interception of data under limited circumstances.

Act 1038 makes provision for certain authorized persons to apply to the courts for a production order to collect subscriber information or for an interception warrant to collect or record traffic data or content data stored in real time.

Applications made in this regard must indicate the measures to be taken to ensure that the data will be procured:

- whilst maintaining the privacy of other users, customers and third parties; and
- without the disclosure of the traffic data of any party not part of the investigation.

DEFINITIONS

- **Data** means information which (a) is processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record.
- **Data controller** means a person who either alone, jointly with other persons or in common with other persons or as a statutory duty determines the purposes for and the manner in which personal data is processed or is to be processed.
- **Data processor** in relation to personal data means any person other than an employee of the data controller who processes the data on behalf of the data controller
- **Data subject** means an individual who is the subject of personal data.
- **Data supervisor** means a professional appointed by a data controller in accordance with section 58 to monitor the compliance by the data controller in accordance with the provisions of the Act.
- **Processing** means an operation or activity or set of operations by automatic or other means that concerns data or personal data and the:
    - collection, organisation, adaptation or alteration of the information or data;
    - retrieval, consultation or use of the information or data;
    - disclosure of the information or data by transmission, dissemination or other means available, or
    - alignment, combination, blocking, erasure or destruction of the information or data.

Definition sensitive personal data

The Data Protection Act does not make provision for 'sensitive personal data'. However 'special personal data', is defined as personal data which relates to:

- the race, colour, ethnic or tribal origin of the data subject;
- the political opinion of the data subject;
- the religious beliefs or other beliefs of a similar nature, of the data subject;
- the physical, medical, mental health or mental condition or DNA of the data subject;
- the sexual orientation of the data subject;
- the commission or alleged commission of an offence by the individual; or
- proceedings for an offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in the proceedings.

NATIONAL DATA PROTECTION AUTHORITY

Data Protection Commission ('Commission')

Pawpaw Street
East Legon
Accra
Ghana
GPS: GA-414-1469

P.O. Box CT7195
Accra
Ghana

Tel: +233-(0)30 2222 929
Email: info@dataprotection.org.gh

REGISTRATION

A data controller who intends to process personal data is required to register with the Data Protection Commission. A data controller who is not incorporated in Ghana must register as an external company.

Upon registration, a data controller is issued a Certificate of Registration which is valid for two (2) years and must be renewed thereafter. The Data Protection Commission also maintains an online public search register of registered data controllers, which shows the status of the entity with the Commission as well as the expiry date of its current registration.

DATA PROTECTION OFFICERS

There is no specific requirement to appoint a data protection officer. However, under the Data Protection Act, 2012 (Act 843) a data controller may appoint a certified and qualified data supervisor to act as a data protection supervisor. The data protection supervisor is responsible for monitoring the data controller’s compliance with the provisions of the Data Protection Act. A person shall not be appointed as a data protection supervisor unless the person satisfies the criteria set by the Data Protection Commission.

COLLECTION & PROCESSING

Collection

A person shall collect data directly from the data subject unless:

- the data is contained in a public record;
- the data subject has deliberately made the data public;
- the data subject has consented to the collection of the information from another source;
- the collection of the data from another source is unlikely to prejudice a legitimate interest of the data subject;
- the collection of the data from another source is necessary for a number of expressly designated purposes (for example the detection or punishment of an offence or breach of law);
- compliance would prejudice a lawful purpose for the collection;
- compliance is not reasonably practicable.

A data controller must also ensure that the data subject is aware of:

- the nature of the data being collected;
- the name and address of the person responsible for the collection;
- the purpose for which the data is required for collection;
- whether or not the supply of the data by the data subject is discretionary or mandatory;
- the consequences of failure to provide the data;
- the authorized requirement for the collection of the information or the requirement by law for its collection;
- the recipient of the data;
- the nature or category of the data;
- the existence of the right of access to and the right to request rectification of the data collected before the collection.

Where collection is carried out by a third party on behalf of the data controller, the third party must ensure that the data subject has the information listed above.

Processing

A person who processes personal data shall ensure that the personal data is processed:

- without infringing the privacy rights of the data subject;
- in a lawful manner; and
- in a reasonable manner.

Under the Data Protection Act, a data controller or is required to ensure that personal data in respect of foreign data subjects is processed in compliance with data protection legislation of the foreign jurisdiction of that subject where personal data originating from that jurisdiction is sent to Ghana for processing.

TRANSFER

There are no specific provisions in the Act on the transfer of personal data. However, the sale and purchase of personal data or information is prohibited. Additionally, a person is prohibited from knowingly obtaining or knowingly or recklessly disclosing the personal data or the information contained in the personal data of another person.

A person who sells or offers to sell the personal data of another person commits an offence and is liable on summary conviction to a fine of not more than 2500 penalty units or to a term of imprisonment of not more than five years or to both.

A person who purchases, knowingly obtains, or knowingly or recklessly discloses personal data is liable on summary conviction to a fine of not more than 250 penalty units or to a term of imprisonment of not more than 2 years or to both.

A penalty unit is equivalent to GHS12 (approximately USD11.6 as at 22 December 2023).

SECURITY

- A person who processes data shall take into account the privacy of the individual by applying the data security safeguards.
- A data controller has an obligation to ensure that a data processor who processes personal data for the data controller, establishes and complies with the security measures provided for under the Act.

BREACH NOTIFICATION

Where there are reasonable grounds to believe that the personal data of a data subject has been accessed or acquired by an unauthorised person, the data controller or a third party who processes data under the authority of the data controller shall notify the Commission and the data subject of the unauthorised access or acquisition as soon as reasonably practicable after the discovery of the unauthorised access or acquisition of the data. The data controller shall take steps to ensure the restoration of the integrity of the information system.

The data controller shall delay the notification to the data subject where the security agencies or the Data Protection Commission inform the data controller that the notification will impede a criminal investigation.

ENFORCEMENT

Where the Commission is satisfied that a data controller has contravened or is contravening any of the data protection principles, the Commission shall serve the data controller with an enforcement notice to require the data controller to do any of the following:

- to take or refrain from taking the steps specified within the time stated in the notice;
- to refrain from processing any personal data or personal data of a description specified in the notice;
- to refrain from processing personal data or personal data of a description specified in the notice for the purposes specified or in the manner specified after the time specified.

A person who fails to comply with an enforcement notice commits an offence and is liable on summary conviction to a fine of not more than one hundred and fifty penalty units or to a term of imprisonment of not more than one year or to both. A penalty unit is equivalent to GHS 12 (approximately USD 2.20).

Further, an individual who suffers damage or distress through the contravention of the data protection obligations by a data controller is entitled to compensation from the data controller for the damage or distress notice.

In October 2020, the Data Protection Commission announced its implementation of an Enhanced Registration and Compliance Software to streamline the registration and renewal process for Data Controllers. There was also announced an extension of the transitional period under the Act during which existing Data Controllers were required to register with the Commission by six months (from 1st of October 2020 to 31st March 2021). During this period, it is reported that defaulting Data Controllers will be required to pay only the current year’s registration fee, with all fees for previous years (up to 2012) in which they were to register but defaulted, waived. Pursuant to the Act however, such extensions of the transitional period are required to be made by a Legislative Instrument, however our checks show that no Legislative Instrument has been passed for this purpose.

A penalty unit is equivalent to GHS12 (approximately USD11.6 as at 22 December 2023).

The Data Protection Commission requires all large data controllers[1] to have a certified data protection supervisor who has undergone training with the Commission. Where a data controller is renewing their license with the Commission, they are required to provide a Gap Analysis report which shows how the data controller has complied with the law and requirements of the Commission as well as areas for improvement. The Gap Analysis is usually done by the data protection supervisor; however, this can be done by a third party who has been certified by the Data Protection Commission. As part of the gap analysis, the data controller will be required to produce a data protection policy, a data protection impact assessment, a data retention policy, an incident report plan, as well as a breach report which should include all breaches no matter the magnitude. Data Controllers are also required to provide regular training, at least once every year, for anyone that deals with personal information on behalf the data controller.

1: Primary criterion: Data controllers with an annual turnover of GHS 5 million (approximately USD 430,337) and above; or minimum of 250 members or staff. Secondary criterion: Specialist industries no matter their turnover; specifically, upstream and midstream petroleum companies, telecommunication companies or operators (Class 1 license operators), banking / financial institution, credit bureaus, insurance companies, mining companies except quarries, members of groups of companies no matter their turnover which has one associate or subsidiary qualifying as a large data controller.

ELECTRONIC MARKETING

The Act prohibits a data controller from using, obtaining, procuring or providing information related to a data subject for the purpose of direct marketing without the prior written consent of the data subject. However, there are no specific provisions that relate to electronic marketing specifically.

ONLINE PRIVACY

The Data Protection Commission shall not grant an application for registration as a data controller where the appropriate safeguards for the protection of the privacy of the data subject have not been provided by the data controller.

The Cybersecurity Act, 2020 (Act 1038) Act 1038 makes provision for certain authorized persons (as specified below) to apply to the High Court for a production order to collect subscriber information[1] or for an interception warrant to collect or record traffic data[2] or content data[3] stored in real time.

An investigative officer[4] who makes an application for a production order to collect subscriber information must demonstrate to the satisfaction of the Court that there are reasonable grounds to believe that the subscriber information associated with a specified communication and related to or connected with a person under investigation is reasonably required for the purpose of a specific criminal investigation.

A senior investigative officer[5] who makes an application to the Court for an interception warrant to collect or record traffic data stored or in real-time must demonstrate to the satisfaction of the court that there are reasonable grounds to believe that the traffic data is required for the purposes of a specific criminal investigation.

A designated officer who makes an application to the Court for an interception warrant to collect or record content data shall demonstrate to the satisfaction of the Court that there are reasonable grounds to authorise the interception of content data and associated traffic data, related to or connected with a person or premises under investigation for one of the following purposes:

- in the interests of national security;
- the prevention or detection of a serious offence;
- in the interests of the economic well-being of the citizenry, so far as those interests are also relevant to the interests of national security; or
- to give effect to a mutual legal assistance request.

Applications made in this regard must indicate the measures to be taken to ensure that the data will be procured:

- whilst maintaining the privacy of other users, customers and third parties; and
- without the disclosure of the subscriber information, traffic data or data of any party not part of the investigation.

1: Act 1038 defines "subscriber information" as any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of the services of a service provider other than traffic or content data and by which may be established (a) the type of communication service used, the technical provisions taken in respect of the communication service and the period of service; (b) the identity, postal or geographic address, telephone and other access number of the subscriber, billing and payment information available on the basis of the service agreement or arrangement; and (c) any other information on the site of the installation of a communication equipment, available on the basis of the service agreement or arrangement;

2: Pursuant to Act 1038 “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the origin, destination, route, time, date, size or duration of the communication or the type of underlying service;

3: Pursuant to Act 1038 “content data” means the communication content of the communication, that is, the meaning or purport of the communication, or the message or information being conveyed by the communication other than traffic data.

4: Pursuant to Act 1038 “investigative officer” means an officer of a law enforcement agency established by law.

5: Pursuant to Act 1038 “designated officer” means any of the following persons: (a) the Director-General of the Bureau of National Investigations; (b) the National Security Coordinator; (c) the Inspector-General of Police; (d) the Commissioner-General of the Ghana Revenue Authority; (e) the Director-General, Defence Intelligence;(f) the Executive Director, Economic and Organised Crime Office; (g) the Director-General, Narcotics Control Commission; (h) the Comptroller-General, Immigration Service; (i) the Director-General, Research Department of the Ministry of Foreign Affairs; (j) the Chief Executive Officer of the Financial Intelligence Centre; or (k) the Attorney-General, acting upon the request of a competent authority of a foreign country.

KEY CONTACTS

Reindorf Chambers
www.reindorfchambers.com

Kizzita Mensah
Partner
Reindorf Chambers
T +233 302 225 674
kizzita.mensah@reindorfchambers.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

GIBRALTAR

Last modified 19 January 2024

LAW

Following the UK’s exit from the European Union, Gibraltar ceased to be a territory within the European Union as of midnight 31st December 2020. As a consequence, the Gibraltar Government transposed the General Data Protection Regulation (Regulation (EU) 2016/679) into Gibraltar national law (thereby creating the “**Gibraltar GDPR**”). In so doing, Gibraltar made number of technical changes to the GDPR to account for its status as a national law of Gibraltar. The Gibraltar GDPR replaces EU terminology with domestic equivalents (e.g. references to “Member State law” become references to “Gibraltar law” and references to “a third country” to “a country or territory outside of Gibraltar”. These changes were made under Gibraltar’s Data Protection, Privacy and Electronic Communications (Amendments Etc) (EU) Exit Regulations 2019.

All material GDPR obligations on controllers and processors remain the same under the Gibraltar GDPR.

Additionally, Gibraltar’s Data Protection Act 2004 (“DPA04) remains in place as a national data protection law, and supplements the Gibraltar GDPR. It deals with matters that were previously permitted derogations and exemptions from the EU GDPR (for example substantial public interest bases for the processing of special category data, and context-specific exemptions form parts of the GDPR such as subject rights).

In addition:

- Part III of the DPA04 transposes the Law Enforcement Directive ((EU) 2016/680) into Gibraltar law, creating a data protection regime specifically for law enforcement personal data processing: and
- Parts V and VI set out the scope of the Information Commissioner's mandate and his enforcement powers, and creates a number of criminal offences relating to personal data processing.

Territorial Scope

Primarily, the application of the Gibraltar GDPR turns on whether an organization is established in GibraltarAn 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in Gibraltar.

However, the Gibraltar GDPR also has extra-territorial effect. An organization that it is not established within Gibraltar will still be subject to the Gibraltar GDPR if it processes personal data of data subjects who are in Gibraltar where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in Gibraltar or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within Gibraltar.

DEFINITIONS

Definition of personal data

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "**identifiable**" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The Gibraltar GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The Gibraltar GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the Gibraltar GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

"Public authority" and "public body" are expressions used in the Gibraltar GDPR. For the purposes of Gibraltar, the DPA04 defines them in S.9.

The DPA04 also clarifies that, where the purpose and means of processing are determined by an enactment of law, then the person on whom the obligation to process the data is imposed by the enactment is the controllerBottom of Form.

Definition of sensitive personal data

Definition of personal data

Any information relating to a Data Subject; and a Data Subject means a natural person who is the subject of Personal Data.

Definition of special category personal data

Information about racial or ethnic origin, religious or philosophical beliefs, trade union membership, health or sex life. The DPA04 also includes a definition on criminal convictions and offences data to include personal data relating to the alleged commission of any offence and information on any proceedings for offences or alleged offences, the disposal of such proceedings and any sentence given.

NATIONAL DATA PROTECTION AUTHORITY

Gibraltar’s Information Commissioner (whose functions are discharged through the Gibraltar Regulatory Authority ("**GRA**")) is the supervisory authority for Gibraltar for the purposes of Article 51 of the Gibraltar GDPR. Following Brexit the GRA will no longer be a competent supervisory authority for the purposes of the EU GDPR. The Gibraltar GDPR also omits Chapter 7 (Cooperation and Consistency) of the EU GDPR, on the basis that Gibraltar will not be part of the EU’s cooperation and consistency mechanisms.

The GRA's contact details are:

Information Commissioner

Gibraltar Regulatory Authority
Suite 603 Europort
Gibraltar

T 200 74636
F 200 72166

info@gra.gi

REGISTRATION

Currently there are no registration requirements for controllers or processors under the Gibraltar GDPR.

There remains however the obligation to register Data Protection Officers with the GRA although no fee is required.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in Gibraltar GDPR, include (Article 39):

- to inform and advise on compliance with Gibraltar GDPR and other Gibraltar data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");

- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the Gibraltar GDPR. Organisations must not only comply with the Gibraltar GDPR but also be able to demonstrate compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Gibraltar law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Schedule 1 to the DPA04 supplements the requirements for processing special categories of personal data, and also provides for a number of ‘substantial public interest’ grounds that can be relied upon to process special categories of personal data in specific contexts which are deemed to be in the public interest. Many of these grounds are familiar from the previous UK law, whilst other are new. Important examples include:

- processing required for employment law;
- heath and social care;
- equal opportunity monitoring;
- public interest journalism;
- fraud prevention;
- preventing / detecting unlawful acts (e.g. money laundering / terrorist financing);
- insurance; and
- occupational pensions.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by domestic law (Article 10). Part 3 of Schedule 1 of the DPA authorises a controller to process criminal conviction or offences data where the processing is necessary for a purpose which meets one of the conditions in Parts 2 of Schedule 1 (this covers the conditions noted above other than processing for employment law, health and social care), as well as number of other specific conditions:

- consent;
- the protection of a data subject's vital interests; and
- the establishment, exercising or defence of legal rights, the obtaining of legal advice and the conduct of legal proceedings

Appropriate policy and additional safeguards

In any case where a controller wishes to rely on one of the DPA04 conditions to lawfully process special category, criminal conviction or offences data, the DPA04 imposes a separate requirement to have an appropriate policy document in place and apply additional safeguards to justify the processing activity. The purpose of the policy document is to set out how the controller intends to comply with each of the data protection principles in Article 5 of the Gibraltar GDPR in relation to this more sensitive processing data activity.

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data – i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The Gibraltar GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose;
- the context in which the data have been collected;
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible);
- the possible consequences of the new processing for the data subjects;
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation.

Transparency (Privacy Notices)

The Gibraltar GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of Gibraltar GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, replicating those in the EU GDPR. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "which produces legal effects concerning [the data subject]… or similarly significantly affects him or her" is only permitted where:

- necessary for entering into or performing a contract;
- authorised by Gibraltar law; or
- the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Child's consent to information society services (Article 8)

Article 8(1) of the Gibraltar GDPR stipulates that a child may only provide their own consent to processing in respect of information society (primarily, online) services, where that child is over 16 years of age, unless Gibraltar applies a lower age. The DPA04 reduces the age of consent for these purposes to 13 years for Gibraltar.

Automated Decision Making (Article 22)

Automated decision making (including profiling) "which produces legal effects concerning [the data subject]… or similarly significantly affects him or her" is only permitted where:

- necessary for entering into or performing a contract;
- authorised by Gibraltar law; or
- the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view. Further safeguards for automated decisions that are necessary for entering into or performing a contract or which are authorised by Gibraltar law are set out in section 17 of the DPA04.

TRANSFER

Transfers from Gibraltar

Transfers of personal data by a controller or a processor to third countries outside of Gibraltar are only permitted where the conditions laid down in Chapter V of the Gibraltar GDPR are met (Article 44).

Article45(1) allows transfers of personal data to:

- third countries on the basis of UK adequacy regulations made under UK GDPR and Part 2 of the UK Data Protection Act 2018; and
- to the United Kingdom.

Currently, the following countries or territories enjoy UK adequacy decisions (these have all essentially been ‘rolled over’, on a temporary basis, from the EU GDPR with some additions): Andorra, Argentina, Canada and Japan (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay, South Korea and New Zealand. Also included are transfers to the USA, if covered under the UK extension to the EU-US Data Privacy Framework.

The UK is also currently treating all EU and EEA Member States as adequate jurisdictions. Therefore transfers to any of the above jurisdictions from Gibraltar will not require any additional safeguards Gibraltar GDPR.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available (Article 46). The list of appropriate safeguards includes, amongst others, binding corporate rules and the use of standard contractual clauses with additional safeguards to guarantee an essentially equivalent level of protection to data subject’s and their personal data.

Section 128A of the DPA04 allows Gibraltar’s Information Commissioner to publish standard data protection clauses which comply with Article 46 requirements. To date, a bespoke International Data Transfer Agreement (“**IDTA**”) has been published for data exports from Gibraltar in addition to an International Data Transfer Addendum (“**Addendum** ”). Both the IDTA and Addendum can be used. Whereas the IDTA is a full-form standalone agreement, the Addendum is to be used along-side the EU Standard Contractual Clauses for use in the context of the Gibraltar GDPR.

Article 49 of the UK GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

- explicit informed consent has been obtained;
- the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between
- the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
- the transfer is made from a register which according to domestic law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to Gibraltar’s Information Commissioner and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside Gibraltar t(Article 48) are only recognised or enforceable (within Gibraltar) where they are based on an international agreement which applies to Gibraltar such as a mutual legal assistance treaty in force between the requesting third country and Gibraltar ; a transfer in response to such requests where there is no other legal basis for transfer will infringe the Gibraltar GDPR.

Transfers from the UK to Gibraltar

Gibraltar and the UK enjoy the free flow of personal data without the need for any additional safeguards.

ibraltar is now a third country for the purposes of Chapter V of the EU GDPR. Unlike the UK, Gibraltar does not currently benefit from an EU adequacy decision. It is expected that Gibraltar will obtain EU adequacy with the conclusion of the UK-EU treaty on Gibraltar. Until then, alternative EU GDPR Chapter V safeguards are required to transfer personal data from the EU to Gibraltar.

SECURITY

The GDPR is not prescriptive about specific technical standards or measures. Rather, the Gibraltar GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the Gibraltar GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

BREACH NOTIFICATION

The Gibraltar GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

Mandatory breach notification

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

Personal data breaches should be notified to GRA as Gibraltar's supervisory authority. Breaches must be reported to the GRA using their Data Breach Notification Form available on their website and sent by email to dpbreach@gra.gi.

ENFORCEMENT

Fines

The Gibraltar GDPR empowers the Information Commissioner to impose fines of up to 4% of annual worldwide turnover, or £17.5 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to £17.5 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

The Information Commissioner is not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

The information Commissioner also enjoys a wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The Gibraltar GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the Gibraltar GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with the Information Commissioner (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The DPA04 sets out the specific enforcement powers provided to the GRA pursuant to Article 58 of the GDPR, including:

- information notices – requiring the controller or processor to provide the GRA with information;
- assessment notices – permitting the GRA to carry out an assessment of compliance;

- enforcement notices – requiring the controller or processor to take, or refrain from taking, certain steps; and
- penalty notices – administrative fines.

The Information Commissioner has the power to conduct a consensual audit of a controller or a processor, to assess whether that organisation is complying with good practice in respect of its processing of personal data.

Under Schedule 15 of the DPA04 the Information Commissioner also has powers of entry and inspection. These will be exercised pursuant to judicial warrant and will allow the Information Commissioner to enter premises and seize materials.

The DPA04 creates two new criminal offences in Gibraltar law: the re-identification of de-identified personal data without the consent of the controller and the alteration of personal data to prevent disclosure following a subject access request under Article 15 of the GDPR. The DPA04 retains existing Gibraltar criminal law offences, e.g. offence of unlawfully obtaining personal data.

The DPA04 requires the Information Commissioner to issue guidance on its approach to enforcement, including guidance about the circumstances in which it would consider it appropriate to issue a penalty notice, i.e. administrative fine.

The DPA04 also allows the Information Commissioner to publish statutory codes of practice on direct marketing and data sharing.

ELECTRONIC MARKETING

The Gibraltar GDPR applies to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing is consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the Gibraltar GDPR are to be noted, and marketing consent forms invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local law under the Communications (Personal Data and Privacy) Regulations 2006 (the Regulations). EU Member States are supposed to replace the ePrivacy Directive with a Regulation. However, there is still no certainty when this is going to happen. Should this happen, Gibraltar will likely need to adopt any such legislation into its own domestic law.

In the meantime, Gibraltar GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the Gibraltar GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive have been replaced with the Gibraltar GDPR standard for consent.

The Regulations apply to most electronic marketing activities. The Regulations do not prohibit the use of personal data for the purposes of electronic marketing but provides individuals with the right to ‘opt-out’ for direct marketing purposes.

There are a number of different opt-out schemes / preference registers for different media types. Individuals (and, in some cases, corporate subscribers) can contact these schemes and ask to be registered as not wishing to receive direct marketing material. If advertising materials are sent to a person on the list, sanctions can be levied by the Information Commissioner.

The Regulations also prohibit the use of automated calling systems without the consent of the recipient and the use of unsolicited electronic communications (i.e. by email or SMS text) for direct marketing purposes is also prohibited without prior consent from the consumer unless:

- the consumer has provided their relevant contact details in the course of purchasing a product or service from the person proposing to undertake the marketing;
- the marketing relates to offering a similar product or service; and

- the consumer was given a means to readily 'opt out' of use for direct marketing purposes both at the original point where their details were collected and in each subsequent marketing communication.

Each direct marketing communication must not disguise or conceal the identity of the sender and include the 'unsubscribe' feature referred to above.

The restrictions on marketing by email / SMS only applies in relation to individuals and not where marketing to corporate subscribers.

ONLINE PRIVACY

The Communications (Personal Data and Privacy) Regulations 2006 (the Regulations) deal with the collection of location and traffic data by public electronic communications providers ('CPs') and the use of cookies (and similar technologies).

Traffic Data

Traffic Data held by a CP must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

- it is being used to provide a value added service; and
- consent has been given for the retention of the Traffic Data.

Traffic Data can only be processed by a CP for:

- the management of billing or traffic;
- dealing with customer enquiries;
- the prevention of fraud;
- the marketing of electronic communications services; or
- the provision of a value added service.

Location Data

Location Data may only be processed for the provision of value added services with consent and where the identity of the user is anonymised. CPs are also required to take measures and put a policy in place to ensure the security of the personal data they process.

Cookie Compliance

The use and storage of cookies and similar technologies requires:

- clear and comprehensive information; and
- consent of the website user.

The GRA’s position is positive action e.g. via the use of tick box will be required by the user for the installation of cookies and that pre enabled boxes do not amount to consent. Usual data protection principals of the Gibraltar GDPR also apply.

Note consent is not required for cookies that are used for the sole purpose of carrying out the transmission of a communication over an electronic communications network or where this is strictly necessary for the provision of a service requested by the user.

Enforcement of a breach of the Regulations is dealt with by the Information Commissioner and if found guilty a fine and or imprisonment may be imposed. However an individual may also bring an action for damages in the Supreme Court.

KEY CONTACTS

Hassans

www.gibraltarlaw.com/

Michael Nahon
Partner
T (+350) 200 79000
michael.nahon@hassans.gi

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

GREECE

Last modified 19 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Greek Law 4624/2019 “on the Hellenic Data Protection Authority, the implementation of Regulation 2016/679 and the transposition of Directive 2016/680” (hereinafter the “Law”) (Government Gazette A/137/29.08.2019) was enacted and entered into force in August 28, 2019. The Law regulates the operation of the Hellenic Data Protection Authority, introduces GDPR supplementary rules and transposes the Law Enforcement Directive into Greek Law.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

Definition of supervisory authority

The competent supervisory authority for the territory of Greece is the Hellenic Data Protection Authority (hereinafter the “**HDPA**”).

Definitions as per article 4 of the GDPR

Further to the definitions as per article 4 of the GDPR, the Law provides for specific definitions for the notions of public and private bodies:

- ‘Public body’ means public authorities, independent and regulatory administrative authorities, legal persons governed by public law, first and second-level local government authorities with their legal persons and their legal entities, state-owned or public undertakings and agencies, legal persons governed by private law which are state-owned or regularly receive at least 50% of their annual budget in the form of state subsidies, or their administration is designated by the state;

- ‘Private body’ means any natural or legal person or group of persons without legal personality which does not fall within the definition of a ‘public body’.

Further, as per Law 4961/2022 on “Emerging information and communication technologies, strengthening digital governance and other provisions” the following definitions are worth noting, to the extent related to the data protection regime:

- “Internet of Things” (“IoT”) constitutes any technology that (a) allows devices or a group of interconnected or related devices, through their internet connection, to perform automatic processing of digital data; and (b) enables the collection and exchange of digital data, in order to offer a variety of services to users, with or without human participation.
- “Distributed ledger” is defined as the repository of information that keeps records of transactions, and which is shared and synchronized between a set of DLT network nodes, using a consensus mechanism.
- “Blockchain” is defined as a type of distributed ledger technology that records data in blocks, which are connected to each other in chronological order and form a chain of a consensual, decentralized and mathematically verifiable nature, which is mainly based on the science of cryptography.
- A “smart contract” is defined as a set of coded computer functions, which is finalized and executed through distributed ledger technology in automated electronic form through instructions for the execution of actions, omissions or tolerances, which are based on the existence or not of specific conditions, according to terms recorded directly in electronic code, scheduled commands or programmed language.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Hellenic Data Protection Authority (HDPA)

Kifissias 1-3
115 23 Athens
Greece

T: +30-210 6475600

F: +30-210 6475628

Email: contact@dpa.gr

The HDPA is responsible for supervising the implementation and enforcement of data protection Law in Greece.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

There are no registration requirements under Greek Law. Notification and authorization requirements under the former data protection regime pertaining to the processing of special category data or installation of CCTV systems have been abolished and replaced by the obligation to hold a record of processing activities and to conduct DPIAs.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

Further to the relevant GDPR provisions, the Law lays down specific rules on the appointment of DPO by public authorities. The particularity of Greek law is that public authorities can be considered to be exempted from the obligation to publish the contact details of the DPO and communicate them to the HDPA for reasons of national security or confidentiality.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and

- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to demonstrate compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose;
- the context in which the data have been collected;
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible);
- the possible consequences of the new processing for the data subjects; and
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

- The Law establishes additional purposes in relation to which further processing is allowed.

- With regard to public bodies, processing of personal data for a purpose other than that for which they were collected shall be permitted where such processing is necessary for the performance of the tasks assigned to them and provided that it is necessary:
    - for the verification of the information provided by the data subject because there are reasonable grounds for believing that such information is incorrect;
    - for the prevention of risks to national security, defense or public security, or for securing tax and customs revenue;
    - for the prosecution of criminal offences;
    - for the prevention of serious harm to the rights of another person;
    - for the production of official statistics.

- With regard to private bodies, processing of personal data by private bodies for a purpose other than that for which they have been collected shall be permitted, where necessary:
    - for the prevention of threats to national or public security at the request of a public body; or
    - for the prosecution of criminal offences; or
    - for the establishment, exercise or defense of legal claims, unless the interests of the data subject override the grounds for the processing of those data.

- Data Processing in the Employment context: Βy virtue of the right conferred by Article 88 of the GDPR, the Law lays down detailed sector specific rules in respect for data processing in the context of the employment relationship.

Employee’s personal data can be processed for purposes related to recruitment or the performance of the employment agreement.

Processing of special categories of personal data for employment-related purposes is allowed (i) if necessary to exercise rights or comply with legal obligations derived from labor law or social security and social protection law and (ii) the data controller has no reason to believe that the data subject has an overriding legitimate interest.

Data processing may only exceptionally be based on employee’s consent. Consent may be considered as informed, if the employer has informed the employee about the processing purpose and the right to revoke his / her consent. To assess whether consent is freely given due attention should be paid to the level of dependency of the employee and the conditions under which consent was granted. Consent can be given also by electronic means and should not be tied to the employment agreement. Consent to processing of specific categories of data should be given in relation to said data.

The processing of personal data is also permitted on the basis of collective labor agreements.

Data controllers must take appropriate measures to ensure compliance with the processing principles set forth in Article 5 of the GDPR when processing employees’ data.

Video Surveillance by means of CCTV systems in the workplace is permitted only for reasons of safety and security, provided that employees have been previously informed thereabout. Such data cannot be used for evaluation purposes.

Processing sensitive personal data / consent

- Collection and processing of genetic data for health and life insurance purposes is prohibited under Article 23 of the Law.

- By way of derogation from Article 9 para. 1 of the GDPR, the processing of special categories of personal data within the meaning of Article 9 para. 1 of the GDPR by public and private bodies shall be allowed, if necessary: (a) for the purpose of exercising the rights arising from the right to social security and social protection, and for fulfilling the obligations arising therefrom; (b) for the purposes of preventive medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or the management of health or social care systems or pursuant to a contract with a health professional or other person who is subject to a duty of professional secrecy or supervised by him/her; or (c) for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, in addition to the measures referred to in the second subparagraph of paragraph 3, the provisions ensuring professional secrecy provided for in a law or code of conduct must in particular be complied with. It goes without saying that the processing of special categories of personal data shall be accompanied by the implementation of the appropriate technical and organisational measures.

- By way of derogation from Article 9 para. 1 of the GDPR, the processing of special categories of personal data by public bodies within the meaning of Article 9 para. 1 of the GDPR shall be allowed, where it is: (a) strictly necessary for reasons of essential public interest; (b) necessary for the prevention of major threats to national or public security; or (c) necessary for taking humanitarian action, in which case the interests in the processing override the interests of the data subject.

Further Processing

- With regard, in particular, to public bodies, the processing of special categories of personal data, as referred to in Article 9 para. 1 of the GDPR, for a purpose other than that for which they have been collected, shall be permitted provided that the conditions set out in the paragraph 1 of Art. 24 of Law 4624/2019 are fulfilled and one of the exemptions provided for in Article 9 para. 2 of the GDPR or Article 22 of Law 4624/2019 applies.

  As far as private bodies is concerned, the processing of special categories of personal data, as referred to in Article 9 para. 1 of the GDPR, for a purpose other than that for which they have been collected, shall be permitted, provided that the conditions set out in the paragraph 1 of Art. 25 of Law 4624/2019 are fulfilled and one of the exemptions provided for in Article 9 para. 2 of the GDPR or Article 22 of Law 4624/2019 applies.

- **Processing and Freedom of Expression and Information:** Exercising the discretion under Article 85 GDPR, the Law sets the conditions for data processing that is necessary to uphold the right to freedom of expression and information and precludes in this case the application of the majority of data controller’s obligations.

  To the extent necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression, the processing of personal data is allowed where: (a) the data subject has given his or her explicit consent, (b) it relates to personal data which are manifestly made public by the data subject, (c) the right to freedom of expression and the right to information override the right to the protection of the data subject’s personal data, in particular on matters of general interest or where it relates to personal data of public figures, and (d) where it is limited to what is necessary to ensure freedom of expression and the right to information, in particular with regard to special categories of personal data, criminal proceedings, convictions and related security measures, taking into account the right of the data subject to his or her private and family life.

  To the extent necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression, the following shall not apply: (a) Chapter II of the GDPR (principles), except for Article 5, (b) Chapter III of the GDPR (rights of the data subject), c) Chapter IV of the GDPR (controller and processor), except for Articles 28, 29 and 32, (d) Chapter V of the GDPR (transfer of personal data to third countries or international organisations), (e) Chapter VII of the GDPR (cooperation and consistency) and f) Chapter IX of the GDPR (specific data processing situations)” (Article 28 para. 2 of Law 4624/2019).

- **Processing for Archiving, Scientific or Historical Research or Statistical Purposes:** Having regard to the margin of discretion under Article 89 of the GDPR, the Law stipulates the security requirements for processing data for archiving, scientific or historical research or statistical purposes and restricts the scope of data subject’s rights.

  1. By way of derogation from Article 9 para. 1 of the GDPR, special categories of personal data within the meaning of Article 9 para. 1 of the GDPR shall be processed where it is necessary for archiving purposes in the public interest. The controller shall have the obligation to take suitable and specific measures to protect the data subject's legitimate interests.

  In derogation from the provisions of Article 15 of the GDPR the access right of the data subject can be restricted in whole or in part to data related to it, if exercise of the right could possibly hinder the fulfillment of archiving purposes in the public interest (as provided in Art. 29 para. 1 of Law 4624/2019), especially in the case that the archiving material is not kept in relation to the data subject's name and the exercise of the right would require disproportionate efforts (Article 29 para. 2 of Law 4624/2019).

  In derogation from the provisions of Article 16 of the GDPR the data subject does not have the right of rectification of inaccurate data, if its exercise could possibly hinder the fulfillment of archiving purposes in the public interest or the exercise of third parties’ rights (Article 29 para. 3 of Law 4624/2019).

  In derogation from the provisions of Articles 18 para. 1 (a) (b) and (d), 20 and 21 of the GDPR, the data subject’s rights shall be restricted, if these rights could possibly hinder the fulfillment of the specific archiving purposes in the public interest (as provided in Art. 29 para. 1 of Law 4624/2019) and such limitations are considered as necessary for the fulfillment of those purposes (Article 29 para. 4 of Law 4624/2019).

  2. By way of derogation from Article 9 para. 1 of the GDPR, the processing of special categories of personal data, within the meaning of Article 9 para. 1 of the GDPR, shall be allowed without the consent of the data subject where the processing is necessary for scientific or historical research purposes, or for the collection and maintenance of statistical information, and the interest of the controller is overriding the interest of the data subject in not having his or her personal data processed. The controller shall have the obligation to take suitable and specific measures to protect the data subject's legitimate interests.

  By way of derogation form the provisions of Articles 15, 16, 18 and 21 of the GDPR, the rights of the data subject shall be limited where their exercise is likely to render impossible or seriously impair the achievement of the objectives referred to in paragraph 1 and where such limitations are deemed to be necessary for their achievement. For the same reason, the data subject’s right of access provided for in Article 15 of the GDPR shall not apply where personal data are necessary for scientific purposes and the provision of information would entail a disproportionate effort (Article 30 para. 2 of Law 4624/2019).

  In addition to what is referred to in paragraph 1, special categories of personal data, where processed for the purposes of paragraph 1 shall, unless it is contrary to the legitimate interest of the data subject, be anonymised as soon as the scientific or statistical purposes allow. Until then, the characteristics that can be used to match individual details associated with personal or real situations of an identified or identifiable person must be stored separately. These characteristics can only be combined with individual details if required for research or statistical purposes (Article 30 para. 3 of Law 4624/2019).

  The controller may publish personal data processed in the context of research, if the data subjects have given their consent in writing or the publication is necessary for the presentation of the results of the research. In the latter case, the results shall undergo pseudonymisation prior to being published (Article 30 para. 4 of Law 4624 /2019).

Confidentiality and data protection measures as regards Whistleblowing channels

Any processing activity conducted on data collected from whistleblowers shall be carried out in accordance with the GDPR and Law 4624/2019, and shall rely on the legal basis of ensuring compliance with a legal obligation to which the controller is subject (Article 6 (1)(c) of the GDPR), in this case being the establishment of reporting channels and the implementation of the measures necessary for the monitoring of those channels.

Further, companies shall implement the appropriate technical and organizational measures, such as pseudonymisation measures, both at the time of report follow-ups as well as during communication with the competent authorities.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

Τhe Law does not provide for any additional rules on cross-border data transfers.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Greek Law does not provide for additional requirements in relation to security measures other than those set forth in the GDPR. Only with regard to special categories of data, the Law provides an indicative list of the security measures, which should be taken. More specifically, when processing special categories of personal data, appropriate security measures to safeguard the data subject’s interests should be adopted. Such measures may include:

- Technical and organizational measures to ensure that processing complies with the GDPR.
- Measures to verify and establish whether and by which party personal data were fed into, altered or removed.
- Data Protection awareness
- Data classification and access rights
- Designation of a DPO
- Pseudonymization of personal data
- Encryption of personal data
- Measures to restore confidentiality, integrity, availability and resilience of processing systems and services, including the ability to restore availability and access to data in the event of physical or technical incident
- Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Law does not derogate from the provisions of the GDPR.

It is worth noting, however, that it provides for an additional exception from the obligation to communicate data breaches to the data subject under Article 34 GDPR. Article 33 (5) of the Law provides that in addition to the exception established in Article 34 (3) GDPR, the obligation to communicate a personal data breach to the data subject does not apply when such notification would lead to disclosure of information which must be kept confidential by operation of law or due to their nature, unless the data subject’s interests take precedence.

Further, according to the Hellenic Data Protection Authority (“**HDPA**”), the procedure to be followed for a Data Breach Notification is the following:

- The Controller may complete the relevant form and submit it to the HDPA electronically via its web portal;
- By way of exception, as regards entities that are not established in Greece, the notification of the data breach procedure may be made via email.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;

- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss;
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Administrative fines

The HDPA may impose administrative fines in accordance with article 83 para. 4 and 5 of the GDPR. The acts of the DPA through which administrative fines are imposed, constitute enforceable deeds and shall be served to the data controller, the data processor or their representatives. Such fines shall be collected according to the Public Income Collection Code.

It is worth noting that the largest fine issued to date by the HDPA amounts to EUR 20 million whilst the total value of all fines issued to date amounts to over EUR 32 million.

Penalties

In exercise of the discretionary powers recognized to Member States by Article 84 of the GDPR, the Law stipulates criminal sanctions which may be applied for unauthorized processing:

- Any act of unauthorized data processing (i.e. access, disclosure, destruction or damage collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction) may lead to imprisonment of up to 1 year.
- If the above mentioned actions relate to special categories of data or data relating to criminal convictions, and offences or related security measures, they are punishable by imprisonment of up to 1 year and penalty payment up to 100.000€. Any person who commits the above actions with intent to obtain unlawful advantage or to cause injury amounting to at least 120.000€, is liable to imprisonment of up to 10 years.
- In the event that the above actions threaten democracy or national security, punishment of imprisonment and penalty payment of up to 300.000€ may be applied.

Right to claim compensation

Further to Article 79 (2) of the GDPR, the Law establishes procedural rules with regard to the venue where civil proceedings may be initiated. Claims for damages brought by data subjects against data controllers or processors as a result of a GDPR infringement shall be filed before the civil court of the registered seat of the controller / processor or the court in whose district the data subject has his / her habitual residence.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State.The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Electronic marketing is regulated by Law 3471/2006 ‘for the protection of personal data and privacy in electronic communications’ (the 'Law’), in combination with the general provisions of Law 2472/1997 *‘for the protection of individuals from the processing of personal data’* (the 'Data Protection Act’).

According to the provisions of article 11 of the Law, data processing for electronic marketing purposes is allowed only upon the individuals’ prior express consent. The said article prohibits the use of automated calling systems for marketing purposes to subscribers that have previously declared to the public electronic communications services providers ('CSPs') that they do not wish to receive such calls in general. The CSPs must register these declarations for free on a separate publicly accessible list.

Personal data (such as e-mail addresses) that have been legally obtained in the course of sales of products, provision of services or any other transaction may be used for electronic marketing purposes, without the receiver’s prior consent thereto, provided that the receiver of such email has the possibility to 'opt out' for free to the collection and processing of his/ her personal data for the aforementioned purposes.

Direct marketing emails or advertising emails of any kind are absolutely prohibited, when the identity of the sender is disguised or concealed and also when no valid address, to which the receivers can address requests for the termination of such communications, is provided.

Electronic marketing is regulated by Greek Law 3471/2006 ‘for the protection of personal data and privacy in electronic communications’, which transposes Directive 2002/85/EC into Greek Law, in conjunction with the GDPR.

According to the provisions of article 11 of Greek Law 3471/2006, data processing for electronic marketing purposes is allowed only upon the individuals’ express prior consent. Use of automated calling systems without human intervention for marketing purposes is prohibited in respect of subscribers that have declared to the public electronic communication services providers ('CSPs') that they do not wish to receive such calls.

Where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services, without prior consent, provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

ONLINE PRIVACY

Articles 4 and 6 of the Law (as amended by Directive 2009/136/EC) deals with the collection of location and traffic data by CSPs and the use of cookies and similar technologies.

Traffic data

Traffic data of subscribers or users held by a CSP must be erased or anonymized after the termination of a communication, unless they are retained for one the following reasons:

- The billing of subscribers and the payment of interconnections, provided that the subscribers are informed of the categories of traffic data that are being processed and the duration of processing, which must not exceed 12 months from the date of the communication (unless the bill is doubtable or unpaid).

- Marketing of electronic communications services or value added services, to the extent that traffic data processing is absolutely necessary and following the subscriber’s or the user’s prior express consent thereto, after his / her notification regarding the categories of traffic data that are being processed and the duration of the processing. Such consent may be freely recalled. The provision of electronic communication services by the CSP must not depend on the subscriber’s consent to the processing of his/her traffic data for other purposes (*eg,* marketing purposes).

Location data

Location data may only be processed for the provision of value added services, only if such data are anonymized or with the subscriber’s / user’s express consent, to the extent and for the duration for which such processing is absolutely necessary. The CSP must previously notify the user or the subscriber of the categories of location data that are being processed, the purposes and the duration of the processing as well as of the third parties to which the data will be transmitted for value added services provision. The subscriber’s / user’s consent may be freely recalled and the 'opt-out' possibility must be provided to the subscriber by the CSP free of charge and with simple means, every time he is connected to the network or in each transmission of communication.

Location data processing is allowed exceptionally without the subscriber’s / user’s prior consent to authorities dealing with emergencies, such as prosecution authorities, first aid or fire-brigade authorities, when the location of the caller is necessary for serving such emergency purposes.

Cookie compliance

The use and storage of cookies and similar technologies is allowed when the subscriber / user has provided his express consent, after his / her comprehensive and detailed notification by the CSP. The subscriber’s consent may be provided through the necessary browser adjustments or through the use of other applications.

The latter do not prevent the technical storage or use of cookies for purposes relating exclusively to the transmission of a communication through an electronic communications network or the provision of an information society service for which the subscriber or the user has specifically requested. The Data Protection Authority is the competent authority for the issuance of an Act, which will regulate the ways such services will be provided and the subscribers’ consent will be declared.

Articles 4 and 6 of Greek Law 3471/2006 regulate collection of location and traffic data by CSPs and the use of cookies and similar technologies.

Traffic data

Traffic data held by a CSP must be in principle erased or anonymized upon termination of the communication to which they refer. The aforementioned rule does not apply with regard to traffic data retained for billing, marketing and law enforcement purposes.

Location data

Location data may only be processed for the provision of value added services, only if they are anonymized or upon subscriber’s / user’s express consent, unless processing and disclosure of such data to public authorities is necessary in case of emergency.

Cookies compliance

Rules on use of cookies and similar technologies are set forth in the HDPA Guidance Note on “the use of cookies and other tracking technologies”. The use and storage of cookies and similar technologies is allowed when the subscriber / user has provided his express consent. The subscriber’s consent may be provided by means of cookie pop-up or banners and shall meet GDPR consent requirements.

Use of cookies for purposes relating exclusively to the transmission of a communication through an electronic communications network or the provision of an information society service for which the subscriber or the user has specifically requested, are exempted from aforementioned requirement.

KEY CONTACTS

Kyriakides Georgopoulos Law Firm
www.kglawfirm.gr

Irene C. Kyriakides
Partner
Kyriakides Georgopoulos Law Firm
i.kyriakides@kglawfirm.gr

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

GUATEMALA

Last modified 21 December 2021

LAW

Guatemala does not have a personal data protection law, however the Law on Access to Public Information (*Ley de Acceso a la Información Pública* – Decree 57-2008 of the Congress of the Republic), even if it pertains to information in public files and records, does address the matter in certain provisions which can be applicable to private parties.

DEFINITIONS

Definition of Personal Data

Article 9, number 1 of the Law on Access to Public Information defines Personal Data as *“relative to any information pertaining to natural persons identified or identifiable.”*

Definition of Sensitive Personal Data

Article 9, number 2 of the Law on Access to Public Information defines Sensitive Personal Data as *“such personal data referring to physical or moral characteristic of the persons or to facts or circumstances of its private life or activity, such as personal habits, racial origins, ethnic origin, ideology or political opinions, religious beliefs or convictions, physical or psychologic health status, sexual preference or sex life, moral and familiar situation or other intimate matters similar in nature.”*

NATIONAL DATA PROTECTION AUTHORITY

According to Art. 46 of the Law on Access to Public Information the competence as National Data Protection Authority is the Ombudsman *(Procurador de los Derechos Humanos).*

REGISTRATION

Registration of Personal Data is not regulated, yet if personal data of an individual is gathered by any public office or obliged subject, even private parties (under the premise that they receive public funds or grants from the State of Guatemala), Article 30 of the Law on Access to Public Information grants the right to Habeas Data.

DATA PROTECTION OFFICERS

Public offices and private parties defined in Art. 6 of the Law on Access to Public Information must implement Public Information Units, pursuant to Art. 19 of the law.

COLLECTION & PROCESSING

Collection and Processing of personal data is not regulated, however Art. 33 of the Law on Access to Public Information refers files and information systems and Art. 39 refers to electronic or digital records. According to Art. 36 of the Law, all information

in public records must be safeguarded and should not be destroyed. Art. 32 of the Law prohibits the creation of data banks or files containing sensitive data and sensitive personal data, unless such information is for the service and attention of the public institution creating the data bank.

TRANSFER

Transfer of Personal Data is not regulated, however, Art. 31 of the Law on Access to Public Information establishes that written consent is necessary for any type of information transfer and bans expressly the commercialisation of sensitive data and sensitive personal data.

SECURITY

Security is not regulated. However, as referred above, according to Art. 36 of the Law, all information in public records must be safeguarded and should not be destroyed.

BREACH NOTIFICATION

Breach Notification is not regulated, however, Art. 17 of the Law on Access to Public Information stipulates that the person consulting public information must give notice to the relevant authority of the destruction or misuse of public information.

Mandatory breach notification

Mandatory Breach Notification is not regulated.

ENFORCEMENT

According to Arts. 61, 62 and 63 of the Law on Access to Public Information, enforcement corresponds to the Superior Authorities of the relevant public offices and in the event the infraction entails criminal responsibility it corresponds to the Prosecutor General’s Office. Arts. 64 to 67 of the Law specifically create criminal figures related to the abuse and misuse of information contained in public records, including Personal Data.

Specifically, Art. 64 of the Law establishes a prohibition to private parties to commercialise personal data without consent. Violation to this provision results in jail from 5 – 8 years and a fine ranging from Q.50,000.00 to Q.100,000.00 and the confiscation of any element employed to execute the crime.

ELECTRONIC MARKETING

According to the Law of Acknowledgment of Electronic Communications and Signatures, Decree 47-2008 of the Congress of the Republic, electronic marketing is not considered E-Commerce, yet it is considered a communication and an electronic communication as it contains an exposition, statement, claim, advice, request, or offer and the acceptance of an offer, in relation to the construing or execution of a contract.

If any such communication is not addressed to a particular person but it is a general communication, according to Art. 25 of the aforementioned law, it shall be deemed an offer.

Protection to the consumer in E-Commerce and E-Marketing or E-Advertisement is addressed in Art. 51 of the aforementioned law, compelling the originators of such communications to act in an equitable manner and to fully comply with the offered matters and not to engage into false, deceitful, fraudulent or disloyal business practices.

ONLINE PRIVACY

Online privacy is not regulated.

KEY CONTACTS

Central Law
central-law.com/portfolio/central-law-guatemala/

Carlos Cabrera
Associate
Central Law
T +502 23836000
ccabrera@central-law.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

GUERNSEY

Last modified 19 January 2024

LAW

The Data Protection (Bailiwick of Guernsey) Law, 2017 ("**DPL 2017**") came into force on 25 May 2018 to coincide with the enforcement of the EU's General Data Protection Regulation (EU) 2016/670 ("**GDPR**").

Adequacy

The DPL 2017 replaced Guernsey's first set of data protection legislation that was introduced in 2001 in the form of the Data Protection (Bailiwick of Guernsey) Law, 2001, as amended ("**DPL 2001**"). The DPL 2001 had been implemented in response to the EU Directive 95/46/EC. Whereas the DPL 2001 was modelled on a UK enactment, the DPL 2017 is stated to be 'equivalent' to the GDPR.

In 2003 Guernsey was recognised by the European Commission as providing an adequate level of protection for the free flow of personal data to the Bailiwick (see Opinion 02072/07/EN WP 141 and Opinion 10595/03/EN WP 79). Following the enforcement of the GDPR from 25 May 2018, the adequacy decision remains valid and effective in respect of Guernsey's revised data protection regime under the DPL 2017. The adequacy decision is currently being reassessed by the European Commission (as per Article 45(9) GDPR) and confirmation of the outcome of such reassessment was expected during 2021, but this is still awaited.

Scope and applicability

The DPL 2017 applies in relation to the processing of personal data where:

- the processing is by automated means (whether wholly or partly) **OR** if, the processing is not by automated means, it is intended to form part of a filing system; and
- the processing is conducted by a controller or processor established in the Bailiwick of Guernsey ("**Bailiwick**") **OR** the personal data is that of a Bailiwick resident and is processed in the context of the offering good or services (whether or not for payment) to the resident or the monitoring of the resident's behaviour in the Bailiwick. The term "established in the Bailiwick" is defined under the DPL 2017.

In practice, this means that there may be instances where controllers and processors established in the Bailiwick are subject to both the DPL 2017 and, where they process personal data of data subjects who are in the EU, the GDPR.

A domestic exception is available where the processing is for the purpose of an individual's personal, family or household affairs.

As from 25 May 2019, the initial period of transitional relief granted to controllers and processors in Guernsey came to an end. All controllers and processors must therefore comply with all aspects of the DPL 2017 (including the duty to notify pre-collected data, carry out privacy impact assessments, comply with statutory obligations in relation to processor and joint controller-led duties and renew consents collected prior to 25 May 2018).

There is also a requirement (in certain instances) for controllers not 'established in the Bailiwick' to designate and authorise a representative in the Bailiwick.

The Prevention of Discrimination (Guernsey) Ordinance, 2022 is in effect from 1st October 2023 and legislates against discriminating people on the grounds of religion, belief, sexuality, race, disability or carer status. Additional provisions will be coming into effect in 2028. While not directly impacting data protection considerations, it is likely to impact the way in which employers are required to collect and use personal data about potential, new and existing employees. It is also likely to include the processing of special category data. As the impact becomes clear, this will be updated.

DEFINITIONS

Definition of personal data

Section 111(1) of the DPL 2017 defines personal data as "*any information relating to an identified or identifiable individual*".

An 'identifiable individual' is given special meaning under Schedule 9 of the DPL 2017 and is defined as an individual who can be directly or indirectly identified from the information including:

- by reference to a name or an identifier;
- one or more factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity;
- where, despite pseudonymisation, that information is capable of being attributed to that individual by the use of additional information; or
- by any other means reasonably likely to be used, taking into account objective factors such as technological factors and the cost and amount of time required for identification in the light of the available technology at the time of processing.

Definition of special category data

'Special category data' means personal data consisting of information as to a data subject's:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data, meaning personal data relating to the inherited or acquired genetic characteristics of an individual which gives unique information about their physiology or their health, including as a result of an analysis of a biological sample from that individual
- biometric data, meaning personal data resulting from the specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic data
- health data, which includes any personal data relating to the health of an individual, including the provision of health care services, which reveals their health status and includes information about their physical or mental health
- sex life or sexual orientation
- criminal data which relates to the commission or alleged commission by an individual of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

NATIONAL DATA PROTECTION AUTHORITY

Overall oversight of the implementation of the DPL 2017 is vested in the Data Protection Authority ("**Authority**"). The Authority delegates many of the day-to-day regulatory functions and provides governance to an independent operational body known as the Office of the Data Protection Authority ("**ODPA**") (formerly, the Office of the Data Protection Commissioner).

The Authority and the ODPA are also required, pursuant to The Data Protection (International Cooperation and Assistance) (Bailiwick of Guernsey) Regulations, 2018 to have regard to Articles 60 – 62 GDPR by providing mutual cooperation with other supervisory authorities relating to both the GDPR and the DPL 2017.

The office of the data protection authority

St Martin’s House
Le Bordage
St. Peter Port
Guernsey
GY1 1BR

Telephone

+44 (0) 1481 742074

E-mail

enquiries@odpa.gg

Website

odpa.gg

REGISTRATION

Section 39 of the DPL 2017 prohibits all controllers **and** processors established in the Bailiwick from processing personal data unless they have registered with the ODPA. Failure to comply with section 39 of the DPL 2017 is a criminal offence.

The Authority may prescribe the form and manner of registration. These particulars are described in the Data Protection (General Provisions) (Bailiwick of Guernsey) Regulations, 2018 (as amended) (the "**Registration Regulations**")) which set out the framework for a new registration and levy collection regime applicable from 1 January 2021. The new regime abolishes the previous set of exemptions from registration (which expired on 31 December 2020) and replaces them with a much narrower sub-set of exemptions.

The Registration Regulations also introduce the concept of a 'Levy Collection Agent', which is, in essence, a regulated entity licensed by the Guernsey Financial Services Commission (GFSC) who has been appointed to collect an entity's registration fees on its behalf.

Importantly, whilst a Levy Collection Agent has certain responsibilities under the Registration Regulations (which include submitting an annual return, preparing and issuing certificates of exemption to all relevant entities which it administers and retaining records on such entities for a period of 6 years), the ODPA has clarified in its guidance that "*all the legal responsibility as well as liability for data protection compliance still rests with [the controller/processor]…[and in this regard Levy Collection Agents] are simply … a payment gateway to assist with the administrative requirements for the regulated community.*"

Exemptions

Certain limited exemptions to the requirement to register are available to some controllers and processors under the Registration Regulations. These include, for example, where the controller and/or processor has appointed a Levy Collection Agent on its behalf. Not all entities will be eligible to appoint a Levy Collection – this route is only available to organisations who employ fewer than 50 FTE employees, are not required by law to appoint a DPO, do not already act as a Levy Collection Agent and are not nonprofits.

If a controller or processor seeks to rely on any one exemption, they must document their rationale for their decision.

Registration particulars

Since the introduction of the DPL 2017, the ODPA has streamlined the registration regime, both from an outward-facing and internal perspective. For example, in accordance with the GDPR's approach, the register is no longer available to be searched online, thereby removing the requirement for the ODPA to maintain a public register containing significant volumes of processing details. The ODPA has also removed the requirement for controllers and processors to include details about the types of processing undertaken and no longer requires entities to provide a description of the categories of data subject or details of the countries to which such data is transferred.

Instead, at the time of writing, a controller or processor established in the Bailiwick who is required to register with the ODPA must give the ODPA an online annual return setting out the following information (as stipulated in the Registration Regulations):

- the contact details (including name and principal business address) of the entity to be registered
- confirmation of whether the entity is a controller, processor or both in relation to the processing activities
- the representative[1] appointed (if the entity is based outside the Bailiwick)
- confirmation of whether the entity is a charity / not-for-profit
- the DPO (as applicable)
- confirmation of whether the entity employs 50 or more full time equivalent employees
- confirmation of whether the entity has agreed to act as Levy Collection Agent

The return must also be accompanied by a levy, which will be calculated depending on the status of the organisation (i.e. if it is a charity/not for profit) and the number of full-time equivalent employees employed by the entity.

Levy Collection Agents are required to submit a slightly different set of information to the ODPA, as follows:

- the contact details (including name, principal business address and GFSC number) of Levy Collection Agent
- confirmation of whether the entity is a controller, processor or both in relation to the processing activities
- the DPO (as applicable)
- confirmation of whether the entity employs 50 or more full time equivalent employees
- Declaration of the number of organisations the Levy Collection Agent is acting for.

The return must also be accompanied by a levy (being the aggregate of its own fees plus those of the entities that it administers).

There are two levels of fees:

- For organisations with 1-49 full-time equivalent (FTE) employees - £50 per annum; or
- For organisations with 50 or more FTE employees - £2,000 per annum.

The Registration Regulations stipulate separate levies are applicable when dealing with certain government bodies.

---

1. Section 38 of the DPL 2017

DATA PROTECTION OFFICERS

A data protection officer (**"DPO"**) must be appointed where:

- processing is carried out by a public authority (other than a court, or tribunal acting in a judicial capacity); or
- the core processing operations of the controller or processor require or involve "*large-scale and systematic monitoring of data subjects*" or "*large-scale processing of special category of data*".

The ODPA has issued guidance clarifying what is intended by the use of the term "*large-scale processing*", noting that this term is not defined in either the GDPR or the DPL 2017.

The ODPA's guidance references the guidance on the appointment of DPOs ("**DPO Guidelines**") issued by the EU's former advisory body (previously known as the Article 29 Working Party and now replaced by the European Data Protection Board ("**EDPB**")). The ODPA advises controllers and processors to take into account the terms of both the GDPR and the DPO Guidelines when assessing whether or not a DPO is required to be appointed. It also clarifies that small businesses in Guernsey are, as a general rule, unlikely to be undertaking large-scale processing unless they work with large databases of customers or other types of data subjects. Finally, the ODPA expects controllers and processors to review the scope and nature of processing periodically to ascertain whether or not their prior assessment remains valid or if there are sufficient factors to warrant appointing a DPO. All controllers and processors should document their decision-making and the outcome of such reviews.

COLLECTION & PROCESSING

Principles

Data controllers must comply with the data protection principles set out under Section 6(2) DPL 2017 ("**Principles**").

The Principles comprise:

a. **Lawfulness, fairness and transparency**: personal data must be processed lawfully, fairly and in a transparent manner in relation to the data
b. **Purpose limitation**: personal data must be collected for specified, explicit and legitimate purposes and, once collected, not further processed in a manner incompatible with those purposes
c. **Data minimisation**: personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
d. **Accuracy**: personal data must be accurate and, where necessary, kept up to date, with reasonable steps being taken to ensure that personal data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
e. **Storage limitation**: personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed
f. **Integrity and confidentiality**: personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
g. **Accountability**: the controller is responsible for, and must be able to demonstrate compliance with, the data protection principles described under paragraphs (a) – (f) above.

Lawful basis

Data controllers are required to ensure that they have a lawful basis for processing personal data. The DPL 2017 sets out a number of conditions which may be relied upon to legitimise the processing of personal data and special category data.

The most common conditions for controllers to rely on are that:

- the data subject consents to the processing
- the processing is necessary for the performance of a contract to which the data subject is a party or between a controller and a third party in the interests of a data subject, or is in order to take steps at the data subject’s request with a view to entering into a contract
- the processing is necessary for the controller to exercise any right or power, or perform or comply with a duty imposed on it by law, otherwise than an obligation imposed by an enactment, an order, or a judgment of a court or tribunal having the force of the law in the Bailiwick
- the processing is necessary in order to protect the vital interests of the data subject
- the processing is necessary for legitimate interests of the controller or third party except where the processing is exercised by a public authority
- the processing is necessary for the exercise or performance by a public authority of a function that is of a public nature or a task carried out in the public interest.

It is interesting to note that processing in the public interest is only available to public authorities whereas the equivalent provision in the GDPR is much broader than this.

In addition to these conditions, controllers may also rely on one or more of a restrictive set of conditions in order legitimise either personal data or special category data. These include (but are not limited to):

- the data subject providing *explicit* consent to the processing
- processing which is necessary for compliance with a legal right or power or duty imposed on a controller by an enactment
- processing which is made public as a result of steps deliberately taken by the data subject
- processing which is necessary for the purpose of or in connection with legal proceedings, the discharge of any functions of a court or tribunal, obtaining legal advice or establishing, exercising or defending legal rights
- processing which is for the administration of justice of the exercise of any function of the Crown, the States of Guernsey or a public committee
- processing which is necessary for a historical or scientific purpose
- processing is necessary for the vital interests of a data subject.

Additional bases

In addition to the above, further secondary legislation has been adopted which sets out a number of additional lawful bases which are intended to be applied in limited circumstances.

These bases include (but are not limited to):

- the processing of health or criminal data for insurance business purposes
- special category data which is required in order to perform or comply with a duty conferred by law on a controller in connection with employment
- special category data for the prevention, detection or investigation of an unlawful act.

The additional bases will need to be considered on a case-by-case basis and may not always be straightforward to apply. If there were concerns regarding the legitimacy of such processing, we would recommend that you seek Guernsey law advice.

Consent

For the purposes of Section 10 DPL 2017, where a controller seeks to rely on consent, the controller must comply with more stringent requirements than under the DPL 2001 in order to ensure that such consent is valid.

'Valid' consent involves (amongst other characteristics) a "*specific, informed and unambiguous indication of the data subject's wishes by which a data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of their personal data*". In this regard, the DPL 2017 sets the same high standards for consent as the GDPR.

Furthermore, the ODPA guidance confirms that, in addition to the ingredients required to achieve valid consent, explicit consent must be expressly confirmed in words, rather than a positive action. These requirements are summarised in a checklist for controllers setting out what controllers need to do when relying on consent.

Finally in relation to consent, Section 10(2)(f) DPL 2017 stipulates that a child may only provide their own consent to processing in respect of the information society (primarily, online) services, where that child is over 13 years of age. Otherwise, a parent (or other responsible adult) must give it on their behalf.

Transparency

Requirements of transparency under the DPL 2017 closely align with the GDPR. Therefore, the DPL 2017 requires that certain specified information must be supplied as part of a 'fair processing notice' (Schedule 3 DPL 2017), namely:

- the identity and contact details of the controller, and (where applicable), the controller’s representative
- the contact details of the data protection officer (if any)

- confirmation of whether any of the personal data is special category data
- where the personal data is not obtained directly from the data subject: confirmation of the source of the personal data and (if applicable) confirmation of whether the personal data was obtained from a publicly available source and, if so, confirmation of that source
- the purposes for which the data is intended to be processed and the legal basis for the processing
- an explanation of the legitimate interests pursued by the controller or by a third party, if the processing is based on those interests
- the recipients or categories of recipients of the personal data (if any)
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and whether or not there is an adequate level of protection for the rights and freedoms of data subjects
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- information concerning the rights of data subjects
- where the processing is based on consent, the existence of the right to withdraw consent
- a statement of the right to complain to the Authority
- the existence of any automated decision-making, meaningful information about the logic involved in such decision-making and the significance of any such decision making for the data subject
- any further information that is necessary, having regard to the specific circumstances in which the data is or is to be processed, to enable the processing in respect of the data subject to be fair.

Rights of the data subject

The DPL 2017 has strengthened the rights of data subjects in line with the GDPR (Part III DPL 2017).

Controllers must respond to a request "*as soon as practicable*" and in any event within one month following:

- the day on which the controller has received the request,
- the day on which the controller receives the information necessary to confirm the identity of the requestor, or
- the day on which a fee or charge is paid to the controller.

These provisions represent a change to the position as last stated in August 2019 by the UK ICO.

The following rights are available to data subjects:

- *Right to information for personal data collected about the data subject either directly or indirectly (Sections 12-13DPL 2017)*: Where personal data has been collected from a source other than the data subject, certain exceptions are available

- *Right to data portability (Section 14 DPL 2017)*: a data subject has the right to have certain relevant personal data (being personal data relating to that person which has been provided to the original controller directly or via a processor) ported to a new controller, where:

    - that relevant personal data is being processed based on consent; or
    - processing necessary for the conclusion or performance of a contract.

  Where the right applies, the original controller must ensure that any personal data transmitted is provided in a structured, commonly used and machine-readable format. The right is subject to certain exceptions set out under Section 16 DPL 2017

- *Right of access (Section 15 DPL 2017)*: a data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about how the data has been used by the controller. Section 16 DPL 2017 provides for certain exceptions, including where a request cannot be complied with without disclosing information about another individual[1], balancing the rights of the requestor with significant interests of the other individual. The DPL 2017 sets out further detail in respect of the factors which should be taken into consideration when making this determination.

- *Right to object to processing (Section 17 – 19 DPL 2017)*: data subjects have the right to object to processing for: (a) direct marketing purposes, (b) on public interest grounds, and (c) where the processing is for historical or scientific purposes

Whilst the right to object in respect of paragraph (a) is unconditional, the rights to object under paragraphs (b) and (c) are qualified and subject to a public interest test

- *Right to rectification (Section 20 DPL 2017)*: a data subject has a right to request that any inaccurate or incomplete personal data may be corrected or that a statement is provided on the controller's file noting that the data subject disputes the accuracy or completeness of the personal data

- *Right to erasure (Section 21 DPL 2017)*: data subjects may request erasure of their personal data. The right is not absolute; it only arises in a relatively narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or following the successful exercise by the data subject of their right to object or if the data subject withdraws their consent

- *Right to restriction of processing (Section 22 DPL 2017)*: a data subject may request that the processing of their personal data is restricted in certain limited circumstances. Examples include: where the accuracy of the personal data is contested; where the processing is unlawful; or, where the data is no longer required (save for legal claims or for the purposes of obtaining legal advice or establishing / exercising or defending legal rights)

- *Right to notified of restriction, erasure or rectification (Section 23 DPL 2017)*: the controller must not only notify the data subject concerned but, unless it is impracticable or involves disproportionate effort, notify any other person whose personal data has been disclosed

- *Right not to be subject to decisions based on automated processing (Section 24 DPL 2017)*: a data subject has a right not to be subjected to a decision reached through an automated process, and a controller is prohibited from causing or permitting a data subject to be subjected to an automatic decision unless Section 24(2) DPL applies.

Section 24(2) permits automated processing where: the data subject has given their explicit consent, or the processing has been authorised by the States of Guernsey or via an enactment; or, the automated processing is necessary for the vital interests of the data subject or another person or for the performance of a contract.

Additional restrictions apply for the automated processing of special category data. A controller must ensure that appropriate safeguards are in place where automated processing has been conducted in accordance with Section 24(2) DPL (including allowing the data subject to appeal or seek a review of the decision)

- *Right to make a complaint to ODPA (Section 67 DPL 2017)*: a data subject may also complain in writing to the ODPA if they consider that a controller or processor has breached or is likely to breach the DPL 2017 and that breach involves or affects (or is likely to involve or affect) personal data relating to the individual or any data subject right of the individual; and

- *Right to bring a civil action against a controller or processor for breach duty (Section 79 DPL 2017)*: where a controller or processor breaches an operative provision under the DPL 2017 that causes damage to another person, the injured party may bring a claim in tort against the controller or processor for breach of statutory duty. The court may award damages, impose an injunction to restrain an actual or anticipated breach of duty and / or make a declaration that the controller or processor has committed or will commit a breach if its current course of action subsists. Individuals may also claim compensation for distress, inconvenience or other adverse effect suffered by an injured party even if it does not result from any physical or financial loss or damage. Group (or 'class') actions may also be brought against an organisation (Section 97 DPL 2017).

1. It is worth flagging that the DPL 2017 refers to individuals as opposed to the wider concept of 'others', as the equivalent measure is set out in the GDPR. Therefore, it is unclear whether recital 63 of the GDPR would apply in a Guernsey context where the disclosure of information might adversely affect the rights and freedoms of a person other than an individual (e.g. where the disclosure of such information might prejudice the intellectual property rights of a company or partnership).

TRANSFER

The DPL 2017 differentiates between *authorised jurisdictions* and *unauthorised jurisdictions*.

Authorised jurisdictions include:

- the Bailiwick of Guernsey
- a member state of the European Union
- any country, sector or international organisation which has been determined by the European Commission as providing an 'adequate level of protection' for the rights and freedoms of data subjects or
- any *designated jurisdiction*.

A *designated jurisdiction* includes the UK (or any country within the UK), any Crown Dependency (such as the Channel Islands or Isle of Man) or any sector within the UK or a Crown Dependency.

Unauthorised jurisdictions means any countries, sectors in a country or international organisation that does not fall within the scope of an 'authorised jurisdiction'.

Personal data must not be transferred outside of the Bailiwick of Guernsey by a controller or processor ("**Exporter**") to an unauthorised jurisdiction unless the Exporter is satisfied that:

- particular 'safeguards' are in place and there is a mechanism for data subjects to enforce their rights and obtain effective legal remedies against a controller or processor receiving the personal data ("**Importer**") (section 56 DPL 2017)
- the Authority or the ODPA has authorised the transfer (section 57 DPL 2017) or
- other specified *derogations exist* (section 59 DPL 2017)

'*Safeguards*' for the purposes of paragraph (a) above include: legally enforceable agreements (where the Importer is a public authority / body), binding corporate rules, EU's Model Clauses (or equivalent provisions as may from time to time be in force) or approved codes or other approved mechanisms which combine binding and enforceable commitments on the Importer.

'*Derogations*' include:

- the data subject has given explicit consent to the transfer after having been informed of the risks of the transfer
- the transfer is necessary for the performance of a contract between the data subject and the controller or between the controller and third party in the interests of the data subject or for the taking of steps at the request of the data subject with a view to the data subject entering into a contract with the data controller
- the transfer is authorised by regulations made for reasons of public interest
- the transfer is necessary for, or in connection with, legal proceedings, obtaining legal advice or for the purposes of establishing, exercising or defending legal rights
- the transfer is necessary to protect the vital interests of the data subject or another individual (provided that the data subject is physically or legally incapable of giving consent or the controller cannot be reasonably expected to obtain explicit consent)
- the transfer is part of personal data on a public register or a register to which a member of the public has lawful access
- a decision of a public authority (within or without the Bailiwick) based on international agreement imposing international obligations on the Bailiwick or an order of a court or tribunal
- the transfer is in the legitimate interests of the controller which outweighs the significant interests of the data subject and:
    - the transfer is not repetitive

- the transfer only concerns a limited number of data subjects
- the controller has assessed all circumstances surrounding the data transfer and on the basis of that assessment considers that appropriate safeguards to protect personal data have been provided.

Where the transfer is justified on the legitimate interests grounds described above, both the ODPA and the data subject must be notified accordingly.

Guernsey

In common with the GDPR, The DPL 2017 places restrictions on the extent to which personal data may be transferred to recipients outside the Bailiwick of Guernsey ("**Guernsey**").

As set out above, in the absence of an adequacy decision by the EC, transfers are permitted outside the EU/EEA under certain other specified circumstances, in particular where such transfers take place subject to "appropriate safeguards". The Law replicates this regime for transfers outside Guernsey.

Appropriate safeguards for such transfers include:

- Binding corporate rules ("**BCRs**").
- Standard data protection contractual clauses adopted by the European Commission ("**SCCs**").

SCCs are generally the most commonly utilised mechanism for such transfers.

In June 2021, the EC approved a new set of SCCs for international data transfers.[1]

The Guernsey data protection regulator, the ODPA, has now approved the new SCCs for international transfer as a valid transfer mechanism for data transfers from Guernsey (The European Commission’s new Standard Contractual Clauses - technical update ODPA).

The new SCCs for international transfers reflect the changes made to European data protection law made by the GDPR and address some of the issues with the existing sets of SCCs (which include two controller to controller (“**C2C** ”) sets (2001 and 2004) and a controller to processor (“**C2P**”) set (2010). The new SCCs (unlike the existing ones which only applied to C2C and C2P transfers), apply to a broader range of scenarios and include provisions for processor-to-processor ("**P2P**") and processor-to-controller ("**P2C**").

The new SCCs effectively combine all four sets of clauses into one document, allowing controllers and processors to "build" the relevant agreement on a modular basis.

The new SCCs also incorporate provisions to address the Schrems II decision of the European Court of Justice, the key effect of which was to invalidate the EU-U.S. Privacy Shield and to place additional administrative conditions on the use of SCCs.

While a transition period allows businesses to incorporate the old SCCs into new contracts until, at the latest, **27 September 2021**, any Guernsey business looking to export personal data relying on SCCs will after that date need to use the new SCCs which provide for these further steps are taken. All existing contracts must be transitioned to the new SCCs by **27 December 2022**.

Where controllers and processors are utilising SCCs (either new or old) or BCRs, they will need also to take account of the Schrems II decision. The European Data Protection Board ("**EDPB**") has published its Schrems II guidance in relation to supplementary measures to accompany international transfer tools. In summary, a 6 step process is required in relation to international transfers.

1. **Know your transfers.** Be aware of where the personal data so you know the level of protection provided there. Make sure the data you transfer is adequate, relevant and limited to what is.
2. **Verify the transfer tool your transfer relies on**. Using the SCCs or BCRs will be enough in this regard.
3. **Assess** if there is anything in the law and/or practices of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer.

4. **Identify and adopt supplementary measures** necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence. This step is only necessary if your assessment has revealed issues with the third party country's safeguards. If no supplementary measure is suitable, you must avoid, suspend or terminate the transfer.
5. **Take any formal procedural steps** the adoption of your supplementary measure may require.
6. **Re-evaluate at appropriate intervals** the level of protection afforded to the personal data you transfer to third countries and monitor if there have been or there will be any developments that may affect it. This is an ongoing duty.

In practice, the above requires a detailed and documented **transfer impact assessment** ("**TIA**"). For many Guernsey controllers and processors, this will be an onerous process and we would suggest that it should be something that Guernsey businesses should prioritise. We are able to assist clients in this process.

Part of the UK Information Commission consultation on international transfer referenced below includes a TIA toolkit and we would suggest that this provides an excellent and practical starting point for Guernsey controllers and processors

What about the UK?

The European Commission has recognised the UK as an adequate jurisdiction for the purposes of international data transfer, meaning that transfers to and from the UK and Guernsey may continue without restriction.

Guernsey controllers and processors who are subject to the UK GDPR by virtue of its extra territoriality provisions will also need to consider whether they may need to continue using the existing SCCs – the UK is yet to make a decision on replacing them for the purposes of the UK GDPR.

The UK Information Commission has now published a consultation draft of its SCC alternative -– what it describes as an International Data Transfer Agreement ("**IDTA**").

The IDTA looks very different in style to the SCCs and time will tell whether those differences lead to issues between the EU and the UK.

However, it is encouraging to note that the UK's Commission has indicated that for those organisations wishing to use the European Commission approved SCCs, they will be able to do so by completing a straightforward UK addendum.

As noted above, a TIA toolkit is also included.

---

[1] It should be noted that the European Commission also approved a set of SCCs in relation to data processing agreements at the same time.

SECURITY

Security features more prominently under the DPL 2017 than its predecessor. Whilst implementing appropriate security measures to safeguard personal data from unauthorised or unlawful processing continues to be a feature of the DPL 2017 (see Principle 6 'Integrity and Confidentiality'), the DPL 2017 (unlike its predecessor) sets out with more clarity the steps required to ensure compliance.

Data controllers must take reasonable steps to ensure a level of security which is appropriate to the personal data, taking into account the nature, scope, context and purpose of the processing, the likelihood and severity of the risks to data subjects if the personal data is not secure (including the risk of unlawful or accidental destruction, loss or alteration and / or unauthorised disclosure of personal data), best practice and the costs of implementing appropriate measures.

Section 41 of the DPL 2017 provides some assistance as to what may be regarded as a reasonable 'step' to ensure appropriate security. In essence, to ensure compliance with this obligation, a controller should consider:

- pseudonymising and encrypting personal data
- ensuring that the controller or processor has and retains the ability to:

  - ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and
  - restore access to personal data in a timely manner in the event of a physical or technical incident; and
- establishing and implementing a process for regular testing and evaluation of the effectiveness of the technical and organisational measures.

There are several provisions which touch on the security obligations, located throughout the DPL 2017. Thus, the key provisions not only appear in the main security section (Part VI of the DPL 2017) but also form a key consideration (amongst other things) when undertaking a data protection impact assessment, the right to erasure, a controller's duty to take reasonable steps to achieve compliance and the measures that should be in place when choosing a processor. For example, when assessing the suitability of a processor a controller must ensure that the processor provides sufficient guarantees that reasonable technical and organisational security measures governing the processing will be established to meet the requirements of the DPL 2017.

BREACH NOTIFICATION

What is a breach?

The DPL 2017 defines a 'personal data breach' as a "*breach of security leading to the (a) accidental or unlawful destruction, loss, or alteration of; or, (b) unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*".

This definition replicates the definition set out in Article 4 of the GDPR.

Notice to ODPA

As with the GDPR, the DPL 2017 requires all controllers, upon becoming aware of a personal data breach to provide written notice to the ODPA as soon as practicable and no later than **72 hours** after becoming so aware. Section 42(5) of the DPL 2017 provides an exemption from the duty to notify the ODPA where the personal data breach is "*unlikely to result in any risk to the significant interests of the data subject*".

In determining whether or not there is a risk, the ODPA's guidance entitled '*Notification of Personal Data Breaches*' ("**Breach Guidance**") advises organisations who process personal data to consider the type of personal data they hold and whether any breach could, both at the time of the breach and in the future, 'adversely affect an individual' taking into consideration the potential for financial loss, reputational damage, or identity fraud.

The DPL 2017 stipulates the sort of information which must be provided to the ODPA in the event of such a breach including a description of the nature of the personal data breach, contact details of the DPO or contact point, a description of the likely consequences of the breach, a description of the measures taken or proposed to be taken to address risks and mitigate against possible adverse effects and an explanation of any delays (where a breach has been notified after 72 hours).

All breaches which must be notified to the ODPA can be submitted to the ODPA via their online secure breach reporting facility.

In any case, whether a personal data breach is notified to the ODPA or not, the controller must keep a written record of each personal data breach of which the controller is aware, including the facts relating to the breach, the effects, the remedial action taken and any steps taken by the controller to comply with its notification obligations (including a copy of the notice provided to the ODPA).

Notice to data subjects

Where a controller becomes aware of a personal data breach that is likely to pose a "*high risk to the significant interests of a data subject*", the controller must give the data subject written notice of the breach as soon as possible.

The Breach Guidance provides a non-exhaustive of factors for controllers to take into account when determining whether a breach poses a 'high risk'. Whilst financial loss, reputational damage and identity fraud must be considered, the Breach Guidance also includes the risk of whether the breach might have an adverse impact of safety or wellbeing of the data subject (including psychological distress or humiliation). When assessing the risks, the ODPA expects all controllers to consider the nature, scope, context and purpose of the compromised personal data, including whether special category data had been compromised.

Any notice given to an affected data subject must include a description of the nature of the breach, the name and contact details of the DPO or point of contact, a description of the likely consequences of the breach, and a description of the measures taken or proposed to be taken by the controller to address the breach.

A controller is exempt from the requirement to notify a data subject where it has:

- established and carried out appropriate technical and organisational measures to protect personal data and, in particular, those measures have rendered personal data unintelligible to any person who is not authorised to access it (e.g. encryption); or
- taken subsequent measures to mitigate the risk, such that the 'high risk' is no longer likely to materialise, or where the performance of the duty would involve 'disproportionate effort'.

Whilst the Breach Guidance does not define what will amount to 'disproportionate effort to notify', it clarifies that a controller must nonetheless publish a notice (without making public any personal data) or take any other step equivalent to publication in order to inform the data subjects in an equally effective manner.

Notice to controller (where a processor is engaged)

The responsibility for reporting a personal data breach to the ODPA rests with the controller. However, where a processor becomes aware of a personal data breach, the processor must give the controller notice as soon as practicable. Where notice is given orally, written notice must follow at the first available opportunity.

Other regulatory notification requirements

Guernsey's European Communities (Implementation of Privacy Directive) (Guernsey) Ordinance 2004 (as amended) ("**e-Privacy Ordinance**") requires a provider of a public electronic communications service (the '**service provider**') to notify subscribers of a significant risk to the security of the service.

A regulated financial entity must notify the Guernsey Financial Services Commission (the **GFSC**), as soon as reasonably practicable, upon becoming aware of a cyber security event which has resulted in:

- any loss of significant user data;
- significant loss of availability to IT systems;
- significant cost to the business;
- significant loss of business capability;
- significant loss of service to users.

The GFSC does not require licensees to inform them of a data breach unless the data breach is as a result of a cyber security event. However, if a data breach results in the licensee not being able to comply with its regulatory requirements, the GFSC should be notified. Legal advice should be obtained on whether the data breach requires a licensee to notify the GFSC – it may not be required as a matter of course.

ENFORCEMENT

The Authority and the ODPA are responsible for administering and enforcing the DPL 2017 (Section 61(1)(a) DPL 2017).

When investigating a complaint regarding a potential breach of the DPL 2017, the Authority has wide powers to require information and, with appropriate warrants, powers to enter premises and search them (Schedule 7 DPL 2017). It may also conduct and / or require an audit of a controller or processor.

Before making a breach determination or an enforcement order, the ODPA may give the person concerned a written notice of the ODPA's proposals and allow the person time (up to 28 days) to make representations. However, the ODPA may dispense with this requirement if the determination or order needs to be made immediately or without notice in the interests of the data

subjects or where the ODPA has reasonable grounds for suspecting that data may be tampered with or that to do so might seriously prejudice any other investigation etc. There is a right to appeal the decision of the ODPA under section 84 DPL 2017.

Following a breach determination, the ODPA may take the following enforcement action:

Reprimand

The DPL 2017 does not specify the conditions upon which a reprimand may be issued. However, it will most likely take the form of a notice issued in combination with an administrative fine or a formal undertaking by the controller or processor to meet future compliance with any part of the DPL 2018.

Warning

A warning may be given where the ODPA determines that any proposed processing or other act or omission is likely to be a breach of the DPL.

Order

This refers to a formal notice of enforcement and can consist of an order to do any or all of the following:

- bring specified processing operations into compliance with an operative provision of the DPL 2017, or take any other specified action required to comply with said provision, in a manner and within a period specified in the order
- notify a data subject of any personal data breach
- comply with a request made by the data subject to exercise a data subject right
- rectify or erase personal data
- restrict or limit the recipient’s processing operations (which may include restricting or ceasing the processing operation or suspending any transfers to an unauthorised jurisdiction)
- notify persons to whom the personal data has been disclosed of the rectification, erasure or temporary restriction on processing

Administrative fines

Whilst the GDPR has the potential to attract administrative fines of up to 4% of annual worldwide turnover or EUR 20 million (whichever is higher), the administrative fines under the DPL 2017 are generally lower (between £5,000,000 - £10,000,000) and can be broadly categorised on four levels.

Level 1

Administrative fines issued against a controller or processor may not exceed £5,000,000 for breaches of section 74(1)(a) – (d) DPL 2017, comprising the following:

- failure to make reasonable efforts to verify that a person who has given consent to the processing of a child's personal data (being a child who is under 13 years' old) in the context of offering information society services directly to that child, is duly authorised to give consent to that processing under Section 10(2)(f) DPL 2017
- failure to take reasonable steps to inform the data subject of anonymisation (in breach of Section 11(1)(b) DPL 2017)
- any breach of the general duties of controllers and processors (except section 31 DPL 2017 – duty to take reasonable steps for compliance) (breach of Part IV DPL 2017)
- any breach of a controller's administrative duties including the requirement to designate a representative in the Bailiwick in certain cases and the requirement to register and pay fees to the ODPA (as per Part V DPL 2017)
- a breach of the security provisions contained in Part VI DPL 2017
- failure to comply with the requirements in respect of data protection impact assessments and prior consultation (except section 46 DPL 2017 – prior consultation required for high-risk legislation) in accordance with Part VII DPL 2017
- failure to comply with requirements to designate a DPO (where required) or ancillary duties relating to the DPO's functions in accordance with breach of Part VIII of the DPL 2017.

Level 2

Administrative fines issued against a controller or processor may not exceed £10,000,000 for breaches of section 74(1) DPL 2017, comprising the following (in addition to the Level 1 list above):

- breach of any duty imposed on the person concerned by section 6(1) (data protection principles) including lawfulness of processing
- breach of any duty imposed on the person concerned under Part III DPL 2017 (data subject rights)
- failure to comply with an order by the Authority under section 73(2) DPL 2017 within the time specified in the order
- transfer of personal data to a person in an unauthorised jurisdiction in breach of section 55 DPL 2017 (general prohibition of transfers of personal data outside of the Bailiwick to unauthorised jurisdictions)
- breach of any provision of any ordinance or regulations made pursuant to the DPL 2017 which imposes a duty on a controller or processor.

Level 3

In addition to the two administrative fines described above, the DPL 2017 imposes a 'cap' on administrative fines of up to £300,000 (unless the fine is less than 10% of the person's total annual global turnover or total global gross income in the preceding financial year).

Level 4

An administrative fine issued against a person must not exceed 10% of the total global annual turnover or total global gross income of that person during the period of the breach in question, for up to 3 years.

Enforcement activity has increased since the implementation of the DPL 2017 and more specifically during the last 12 months. To date, we are aware that two Guernsey controllers have been subject to administrative fine orders for the sum of £80,000 and £10,000 respectively. We are also aware that the ODPA has issued both public and private reprimands on controllers (the severity of which depends on the seriousness of the breach).

Offences / criminal proceedings

In addition to the above, the DPL 2017 imposes criminal sanctions on persons who are found guilty of certain specified offences. Such offences include:

a. unlawful obtaining or disclosure of personal data
b. obstruction or provision of false, deceptive or misleading information
c. impersonation of an Authority official, and
d. (unless an exception applies) breach of confidentiality by a designated official without the consent of the individual.

Regarding the offence under paragraph (d) above, a 'designated official' shall include a member of the Authority including the Commissioner and any DPO.

Criminal liability can attach to any director or other officer of the organisation including a body corporate, general partner of a limited partnership, foundation official etc. Criminal proceedings may also be instigated against an unincorporated entity in the case of a general partnership, or a committee etc.

ELECTRONIC MARKETING

Direct marketing by electronic means to individuals and organisations is regulated by the European Communities (Implementation of Privacy) Directive (Guernsey) Ordinance 2004 ("**e-Privacy Ordinance**").

Following the implementation of the DPL 2017, minor and consequential changes were made to the e-Privacy Ordinance, which is intended to sit alongside the DPL 2017.

In this regard, neither the e-Privacy Ordinance nor the DPL 2017 prohibit the use of personal data for the purposes of electronic marketing provided that individuals have the right to prevent the processing of their personal data (i.e. a right to 'opt out') for direct marketing purposes.

As such, the e-Privacy Ordinance still reflects the e-Privacy Directive and, for example, prohibits the use of automated calling systems without the consent of the recipient. Furthermore, unsolicited emails can only be sent without consent if:

- the contact details have been provided in the course of a sale or negotiations for a sale
- the marketing relates to a similar product or service, and
- the recipient was given a simple method of refusing the use of their contact details when they were collected.

The identity of the sender cannot be concealed in direct marketing communications sent electronically (which is likely to include SMS marketing).

These restrictions only apply in respect of individuals and not where corporations are sent marketing communications.

ONLINE PRIVACY

The 2011 amendments to the Privacy and Electronic Communications Regulations 2003 by the UK in relation to cookies did not find their way into Guernsey law and there are no immediate plans for this to be done. However, certain aspects of online privacy nevertheless remain governed by the e-Privacy Ordinance (defined under Electronic Marketing above).

As a matter of good practice:

- the use of cookies should be identified to web users
- cookies should be accompanied with a description of what the cookies are doing and why they are being used
- consent should be obtained (at least initially) from the web user where the website intends to store a cookie on their device.

Consent in this context must be freely given, specific, informed and an unambiguous positive action (although it does not need to be explicit).

Traffic data held by a service provider must be erased or anonymised when it is no longer necessary for the purpose of a transmission or communication and only used for permitted purposes. It must also be accompanied by information as to the nature of the processing. Exceptions include if the information is being retained in order to provide a value added service to the data subject or if it is held with their consent.

Traffic data should only be processed by a service provider for (a) the management of billing or traffic, (b) customer enquiries, (c) the prevention or detection of fraud, (d) the marketing of electronic communications services, or (e) the provision of a value added service.

Location data may only be processed in circumstances where the organisation processing such data is a public communications provider, a provider of a value added service, or a person acting on the authority of such provider and only where the user / subscriber cannot be identified from that data (i.e. because they are anonymous) or for the provision of a value added service with consent.

Given the fundamental changes to the data protection regime since the e-Privacy Ordinance was introduced in 2004 and the ongoing negotiations in Europe in relation to the so-called 'e-Privacy Regulation' ("**Regulation**"), further amendments to the e-Privacy Ordinance are, perhaps, inevitable. The States of Guernsey continues to monitor the progress of the draft Regulation in the meantime.

KEY CONTACTS

Carey Olsen (Guernsey) LLP

www.careyolsen.com

Robin Gist
Counsel
Carey Olsen (Guernsey) LLP
T +44 (0)1481 732095
robin.gist@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

GUINEA

Last modified 20 December 2021

LAW

Law n° L/2016/037/AN dated July 28, 2016, on Cybersecurity and Personal Data Protection in the Republic of Guinea regulates personal data.

DEFINITIONS

Definition of personal data

Article 1 of Law No. L/2016/037/AN defines personal data as any information of any kind and regardless of its medium, including sound and image, relating to an identified or identifiable natural person directly or indirectly, by reference to an identification number or to one or more factors specific to his or her physical, physiological, genetic, mental, cultural, social or economic identity.

Definition of sensitive personal data

According to Article 1 of Law No. L/2016/037/AN, sensitive data is all personal data, relating to religious, philosophical, political, trade union opinions or activities, sexual or racial life, health, social measures, prosecution, criminal and administrative sanctions.

NATIONAL DATA PROTECTION AUTHORITY

It is provided for by Article 47 of Law on Cybersecurity and Personal Data Protection in the Republic of Guinea that the authority in charge of personal data protection shall be established by regulatory means. The establishment of this authority is still not effective.

REGISTRATION

Law on Cybersecurity and Personal Data protection in the Republic of Guinea provides that the processing of personal data is subject to a prior declaration or request for authorisation of the competent authority designated by regulation.

The declaration or request for authorisation may be sent to the authority in charge of personal data protection by post, in person at the premises of the said authority or by any other means against the delivery of an acknowledgment of receipt in due form.

The authority in charge of personal data protection has a period of two months to decide on any declaration or request submitted or addressed to it. This period may be extended by two additional months provided that the personal data protection authority can justify its decision or the extension.

The declaration or request for authorisation must include the commitment that the protection meets the requirements of the law on Cybersecurity and Protection of Personal Data and any other regulations or laws in the Republic of Guinea relating to personal data protection.

At the end of this declaration, the competent authority issues a receipt and, if necessary, by electronic means.

The applicant may then implement the processing operation upon receipt of the receipt. However, the applicant is not relieved of any responsibility.

Processing operations carried out by the same organisation and having identical or related purposes may be subject to a single declaration. The information required under the declaration shall be provided for each of the processing operations only insofar as it is specific to said declaration.

Law on Cybersecurity and Personal Data Protection also provides that the modalities for filing declarations or request for authorisation for the processing of personal data shall be determined by presidential decree. This decree has not yet been implemented.

DATA PROTECTION OFFICERS

A data controller will have the option to appoint a data protection officer. According to article 14 and following of Law on Cybersecurity and Personal Data Protection, the data protection officer must be a person qualified to perform such tasks. He must keep a list of the processing operations carried out which is immediately accessible to any person who requests it, and may not be subject to any sanction by his employer as a result of the performance of his duties.

The appointment of a data protection officer by the data controller must be notified to the authority responsible for personal data protection. This appointment must also be brought to the attention of the employer's staff representative bodies.

COLLECTION & PROCESSING

Law on Cybersecurity and Personal Data Protection exempts the processing of personal data from the formalities of declaration, notably in the case of:

- Processing of data used by a natural person exclusively in the course of his or her personal, domestic or family activities;
- Processing of data concerning a natural person, the publication of which is prescribed by a legal or regulatory provision;
- Processing of data whose sole purpose is the keeping of a register which is intended for exclusively private use; etc.

Furthermore, it is also provided that certain matters or actions are subject to prior authorisation by the competent authority before being implemented, these include:

- Processing of personal data relating to genetic and medical data and scientific research in these fields;
- Processing of personal data relating to offences, convictions and security measures pronounced by the competent courts;
- Processing of personal data relating to a national identification number or any other identifier of the same kind, in particular telephone numbers;
- Processing of personal data containing biometric data;
- Processing of personal data for reasons of public interest, in particular for historical, statistical or scientific purposes;
- The proposed transfer of personal data to a third country.

Requests for processing shall be submitted by the controller or his/her legal representative. However, the authorisation does not exempt its holder (data controller) or his representative from their responsibility towards third parties.

TRANSFER

The data controller may be authorised to transfer such data to a third country only if the State ensures a higher or equivalent level of protection of the privacy, fundamental rights and freedoms of individuals with regard to the processing to which such data is or may be subject.

Before any effective transfer of personal data to the third country, the data controller must obtain prior authorisation from the personal data protection authority. Any transfer of personal data to a third country is subject to strict and regular control by the personal data protection authority, in the light of its purpose.

SECURITY

According to Law on Cybersecurity and Personal Data Protection, the processing of personal data is confidential, it must be carried out exclusively by persons acting under the authority of the Data controller, and only on his instructions.

The Data controller is required to take all necessary precautions, in view of the nature of the data, and in particular to prevent it from being distorted, damaged or accessed by unauthorised third parties.

BREACH NOTIFICATION

Law on Cybersecurity and Personal Data Protection provides that the authority in charge of personal data protection may pronounce the following measures against the Data controller:

- A warning to the said controller who does not comply with the obligations resulting from the Law on cybersecurity and Personal Data Protection to which he is subject;
- A formal notice or summons to cease or to cease the breaches noted, within the time limit set by said protection authority.

ENFORCEMENT

Law on cybersecurity and Personal Data Protection sets out administrative, criminal, recidivism and civil liability as well as additional publication of sanctions for breaches of the provisions of said statute.

ELECTRONIC MARKETING

Law L/2016/035/AN on electronic transactions in the Republic of Guinea provides that any advertisement, whatever its form, as soon as it is accessible or likely to be accessible by electronic communications, must be clearly identified as an advertisement. It must also allow the identification and identifiability of the natural or legal person on whose behalf it is made.

Advertisements and notably promotional offers, such as discounts, premiums or gifts, as well as competitions or promotional games, sent by electronic mail, must be clearly, precisely and unequivocally identifiable on the subject of the mail as soon as they are received by the addressee or, if technically impossible, in the body of the message.

The conditions for taking advantage of promotional offers, as well as for participating in promotional courses or games, when offered by e-mail, should be clearly specified and easily accessible to the public.

Pursuant to Law on electronic transactions in the Republic of Guinea, direct marketing by sending messages through an automatic calling machine or SMS, fax or e-mail or any other electronic means of communication using, in whatever form, the contact details of a natural person who has not expressly given his or her prior consent to receive direct marketing through these channels or means is prohibited.

However, direct marketing by e-mail, regardless of the means used, is permitted if:

- The contact details of the recipient of the mail have been collected, with full knowledge of the facts, directly from him/her;
- The direct prospecting is addressed to subscribers or customers of a natural or legal person whose details have been collected with their full knowledge of the facts, for similar products and services that it offers them.

ONLINE PRIVACY

The Law on Cybersecurity and Personal Data Protection does not provide any specific rules governing online privacy.

However, the law prohibits and punishes with a prison sentence of one (1) to five (5) years and a fine of 30,000,000 to 200,000,000 Guinean francs for carrying out or attempting to carry out direct prospecting by any means of communication using, in any form whatsoever, the personal data of a natural person who has not expressed his/her prior written consent.

In particular, it provides that any person has the right to object, on request and free of charge, to the processing of personal data concerning him or her and intended for prospecting purposes.

KEY CONTACTS

Sylla & Partners
syllapartners.com/

Mohamed Sidiki Sylla
Managing Partner
Sylla & Partners
T +224 622 28 10 16
msylla@syllapartners.com

Alpha Toubab Millimono
Associate
Sylla & Partners
T +224 620 56 33 00
amillimono@syllapartners.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

HAITI

Last modified 28 November 2022

LAW

Arrêté fixant les règles relatives à la protection des données à caractère personnel, published in the official gazette, Le Moniteur, #87 of May 15, 2018.

Code Penal, Published in the official gazette, Le Moniteur, Special #10, June 24, 2020.

DEFINITIONS

Definition of Personal Data

There is no definition on the act.

Definition of Sensitive Personal Data

Article 4 of the Decree on personal data provides that *“Any release of personal data that is likely to infringe the rights and freedom of an individual is forbidden”.*

This disposition refers to sensitive personal data according to our interpretation. Thus, sensitive personal data is any data that is likely of infringe the rights and freedom of an individual.

NATIONAL DATA PROTECTION AUTHORITY

Such entity does not exist yet in Haiti.

REGISTRATION

N/A.

DATA PROTECTION OFFICERS

N/A.

COLLECTION & PROCESSING

The person on whom the personal data is collected needs to be informed that it is being collected and will be processed. Collection of personal data needs to relevant and necessary for the purpose of their registration. The purpose of the collection needs to also be communicated to the person.

TRANSFER

If personal data is communicated to a third party, it has to be accessible with the possibility to be modified by the person on which they have been stored.

SECURITY

The Decree provides that the personal data needs to be stored in a way to protect confidentiality and prevent disclosure. When stored, only specific people should have access to them because of their position.

BREACH NOTIFICATION

The law does not regulate how breach of data should be handled. However, any communication of personal data (including breaches) can be subject to criminal and administrative lawsuits.

Mandatory breach notification

No regulation on the matter.

ENFORCEMENT

No specific regulation on that matter.

Article 436, 437 of the Penal Code.

ELECTRONIC MARKETING

The Decree on data privacy requires the user’s consent whereas Article 438 (2) of the Penal Code only specifies that the person needs to opt-out. Given that the Decree on personal data is a specific legislation on data privacy, we recommend having the user consent prior to collecting his data.

ONLINE PRIVACY

No specific regulation on that matter.

KEY CONTACTS

Cabinet Salès
cabinetsales.com/

Christelle Vaval
Partner
Cabinet Salès
T +509 3881 5484
cvaval@cabinetsales.com

Jean-Frédéric Salès
Managing Partner
Cabinet Salès
T +509 2815 1500
jfsales@cabinetsales.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

HONDURAS

Last modified 26 January 2023

LAW

Personal data protection is regulated mainly in:

National Constitution: Article 182 provides the constitutional protection of habeas data, giving individuals the right 'to access any file or record, private or public, electronic or hand written, that contains information which may produce damage to personal honour and family privacy. It is also a method to prevent the transmission or disclosure of such data, rectify inaccurate or misleading data, update data, require confidentiality and to eliminate false information. This guarantee does not affect the secrecy of journalistic sources.'

Law of the Civil Registry (Article 109, Decree 62-2004). This law refers only to public personal information that is contained in the archives of the Civil Registry.

Law for Transparency and for Access to Public Information (Article 3.5, Decree 170-2006). This law enables the access of any person to all the information contained in public entities, except that which is classified as 'Confidential.' It also extends the constitutional protection of habeas data and forbids the transmission of personal information that may cause any kind of discrimination or any moral or economic damage to people.

Rulings on the Law for Transparency and for Access to Public Information (Article 42, Accord 001-2008). Provide a definition of databases containing personal confidential information, and requires data subject consent, prior to the use of it by any third party.

In addition, the Law for the Protection of Confidential Personal Data (the “Law”) is currently in discussion in the Honduran Congress. Congress has approved the first chapters of the Law. The complete approval of the Law and the date for when the Law will enter into force is expected in the first half of 2019.

DEFINITIONS

Definition of personal data

Public Personal Data under the Law of the Civil Registry is defined as: Public Data whose disclosure is not restricted in any way, and includes the following:

- Names and surnames
- ID number
- Date of birth and date of death
- Gender
- Domicile (but not address)
- Job or occupation
- Nationality
- Civil status

Definition of sensitive personal data

The Law for Transparency and for Access to Public Information defines ‘Sensitive Personal Data’ as: "Those personal data relating to ethnic or racial origin, physical, moral or emotional characteristics, home address, telephone number, personal electronic address, political participation and ideology, religious or philosophical beliefs, health, physical or mental status, personal and familiar heritage and any other information related to the honor, personal or family privacy, and self-image."

Other Definitions:

- Consent: Written and express authorization of the person to whom the personal data refers in order to disclose, distribute, commercialize, and/or use it in a different way as it was originally given for
- Confidential Information: Information provided by particular persons to the government which is declared confidential by any law, including sealed bids for public tenders
- Classified Information: Public information classified as that by the law, and / or by resolutions issued by governmental institutions

NATIONAL DATA PROTECTION AUTHORITY

Two entities are responsible for enforcing personal data protection:

1. National Civil Registry
   http://www.rnp.hn

2. Institute for the Access to Public Information
   http://www.iaip.gob.hn

REGISTRATION

Only Obligated Entities must inform the Institute for the Access to Public Information of their databases. Obligated Entities are:

- Government institutions
- NGO’s
- Entities that receive public funds, and
- Trade unions with tax exemptions

The Institute for the Access to Public Information will maintain a list of the databases of the above-mentioned entities.

DATA PROTECTION OFFICERS

Only Obligated Entities must appoint a data protection officer.

COLLECTION & PROCESSING

Individuals, companies, and / or Obligated Entities that collect personal data may not use sensitive personal data or confidential information without the consent of the person to whom such information relates.

However, consent is not required to use or transfer personal data in the following cases:

- If the information is used for statistical or scientific needs, but only if the personal data is provided in a way that it cannot be associated with the individual to whom it relates

- If the information is transmitted between Obligated Entities, only if the data is used in furtherance of the authorised functions of those entities

- If ordered by a Court
- If the data is needed for the purpose it was provided to the individual or company to perform a service. Such third parties may not use personal information for purposes other than those for which it was transferred to them
- In other cases established by law

TRANSFER

Individuals and / or companies may not transfer, commercialize, sell, distribute or provide access to personal data contained in databases developed in the course of their job, except with the express and direct written consent of the person to whom that data refers, subject to certain exceptions.

SECURITY

The Institute for the Access to Public Information has the authority to require all Obligated Entities to take necessary security measures for the protection of the personal data they collect and / or use.

The current legislation neither clarifies nor specifically identifies the security policies or security mechanisms that Obligated Entities must comply with.

As a general statement, the Institute for the Access to Public Information has to ensure the security of all Public Information, of all information classified as confidential by public entities, of all sensitive personal data, and of all information to which the current legislation gives a secrecy status.

BREACH NOTIFICATION

Breach notification is not required.

ENFORCEMENT

The Institute for the Access to Public Information may receive complaints about abuses regarding the collection of personal or confidential data.

The Institute will impose corrective measures and establish recommendations for those persons or companies who disclose personal data, sensitive personal data or confidential data without authorization.

ELECTRONIC MARKETING

There is no law or regulation that specifically regulates electronic marketing.

ONLINE PRIVACY

There is no law or regulation that specifically regulates online privacy.

KEY CONTACTS

Bufete Gutiérrez Falla y Asociados
www.gufalaw.com/

Julio Alejandro Pohl Garcia Prieto
Associate
T +504 2238-2455
julio.pohl@gufalaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

HONG KONG, SAR

Last modified 11 January 2024

LAW

The Personal Data (Privacy) Ordinance (Cap. 486) (**Ordinance**) regulates the collection and handling of personal data. The Ordinance has been in force since 1996, but in 2012/2013 was significantly amended (notably with regard to direct marketing). The Personal Data (Privacy) (Amendment) Ordinance (**Amendment Ordinance**) came into force in October 2021 and introduced new offences of doxxing and corresponding penalties.

At Bill stage, the Amendment Ordinance had originally included a number of other proposed amendments to the Ordinance (as per the January 2020 Consultation Paper), e.g. introducing a mandatory data breach notification mechanism, requiring data users to formulate a data retention policy, empowering the Office of the Privacy Commissioner for Personal Data (**PCPD**) to impose administrative fines linked to annual turnover and regulating data processors directly. According to its report to the Legislative Council in February 2023 (PCPD’s Report), the PCPD is studying further amendments to the Ordinance with the Hong Kong Government to strengthen personal data protection and address challenges including those posed by the internet technology developments.

DEFINITIONS

Definition of personal data

Personal data is defined in the Ordinance as any data:

- Relating directly or indirectly to a living individual;
- From which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
- In a form in which access to or processing of the data is practicable.

The January 2020 Consultation Paper proposed to expand the definition of personal data to cover anonymized information where the relevant individual can be re‑identified.

Definition of sensitive personal data

There is not a separate concept of sensitive personal data in the Ordinance. However, non‑binding guidance issued by the PCPD (in the context of biometric data) has indicated that higher standards should be applied as a matter of best practice to more sensitive personal data.

NATIONAL DATA PROTECTION AUTHORITY

The Office of the Privacy Commissioner for Personal Data (PCPD)

Unit 1303, 13/F, Dah Sing Financial Centre
248 Queen's Road East

Wanchai
Hong Kong

Telephone

+852 2827 2827

Fax

+852 2877 7026

Website

pcpd.org.hk

The PCPD is responsible for overseeing compliance with the Ordinance.

REGISTRATION

Currently, there is no requirement for organizations that control the collection and use of personal data (known as "data users") to register with the data protection authority.

However, under the Ordinance the PCPD has the power to specify certain classes of data users to whom registration and reporting obligations apply. Under the Data User Return Scheme (DURS), data users belonging to the specified classes are required to submit data returns containing prescribed information to the PCPD, which will compile them into a central register accessible by the public. However, at the time of writing, no register has been created to date. The PCPD has proposed to implement the DURS in phases, with the initial phase covering data users from the following sectors and industries:

- the public sector;
- banking, insurance and telecommunications industries; and
- organizations with a large database of members (e.g. customer loyalty schemes).

A public consultation for the DURS by the PCPD was concluded in September 2011. The PCPD had originally planned to implement the DURS in the second half of 2013. However, in January 2014, the PCPD indicated that it planned to put the DURS on hold until the reforms of the European Union (EU) data protection system have been finalized (as the Hong Kong model is broadly based on the same) but no exact time frame for the implementation has been announced. In light of the European Union General Data Protection Regulation 2016/679 (**GDPR**), which generally eliminated the data processing registration requirements under EU data protection law, it is unclear now whether the PCPD will implement the Hong Kong DURS scheme.

DATA PROTECTION OFFICERS

Currently, there is no legal requirement for data users to appoint a data protection officer in Hong Kong. However, the PCPD issued a best practice guide in February 2014 (which was further revised in March 2019) to advocate the development of a privacy management program and encourage data users to appoint or designate a responsible person to oversee the data users' compliance with the Ordinance. There is no specific requirement for a Hong Kong citizen or resident to hold this role. There is no specific enforcement action or penalty if a company does not appoint a data protection officer.

COLLECTION & PROCESSING

A "data user" (which is akin to a "data controller" under GDPR) may collect personal data from a data subject if:

- the personal data is collected for a lawful purpose directly related to a function or activity of the data user;
- the collection is necessary for or directly related to that purpose;
- the data to be collected is adequate but not excessive; and
- all practical steps have been taken to ensure that the data subject has been informed, on or before collection of the data, of the following:

- whether the supply of personal data by the data subject is obligatory or voluntary and, if obligatory, the consequences of not supplying the data;
- the purposes for which the data will be used;
- the persons to whom the data may be transferred;
- the data subject's rights to request for access to and correction of their personal data; and
- the name or job title, and address, of the individual to whom requests for access or correction should be sent.

Separately, additional notice requirements apply to direct marketing (see below).

Data users may only collect, use and transfer personal data for purposes notified to the data subject on collection (see above), unless a limited exemption set out in the Ordinance applies. Any usage or transfer of personal data for new purposes requires the prescribed consent of the data subject.

Data users are also required to take all practicable steps to ensure the accuracy and security of the personal data; to ensure it is not kept longer than necessary for the fulfilment of the purposes for which it is to be used (including any directly related purposes); and to keep and make generally available their policies and practices in relation to personal data.

While the Ordinance currently does not regulate data processors, this was proposed in the January 2020 Consultation Paper and also referred to as an amendment direction in the PCPD’s Report issued in February 2023.

In October 2018, the PCPD published a “New Ethical Accountability framework” Under the framework, the PCPD is effectively urging businesses operating in Hong Kong to undertake privacy impact assessments – referred to as “ Ethical Data Impact Assessments”, which are already required to some extent under a number of other laws, such as China, the Philippines as well as GDPR. In August 2021, the PCPD published the Guidance on the Ethical Development and Use of Artificial Intelligence with the aim to help organizations manage the privacy and ethical risks associated with development and use of Artificial Intelligence.

TRANSFER

Data users may not transfer personal data to third parties (including affiliates) unless the data subject has been informed of the following on or before their personal data was collected:

- that their personal data may be transferred; and
- the classes of persons to whom the data may be transferred.

There are currently no restrictions on transfer of personal data outside of Hong Kong, as the cross‑border transfer restrictions set out in section 33 of the Ordinance were held back and have not yet come into force. A proposal to implement section 33 (perhaps with amendments) was put forward to the Hong Kong Government in 2015, but this process has been delayed. Notably, however, these were not included in the January 2020 Consultation Paper or mentioned in the PCPD’s Report issued in February 2023. If these restrictions come into force as currently drafted, they will have a significant impact upon outsourcing arrangements, intragroup data sharing arrangements, compliance with overseas reporting obligations and other activities that involve cross-border data transfer.

Nevertheless, non‑binding best practice guidance published by the PCPD encourages compliance with the cross‑ border transfer restrictions in section 33 of the Ordinance, which prohibit the transfer of personal data to a place outside Hong Kong unless certain conditions are met (including a white list of jurisdictions; separate and voluntary consent obtained from the data subject; and an enforceable data transfer agreement for which the PCPD provides suggested model clauses). In practice, most data users will enter into data transfer agreements by putting in place the recommended model contractual clauses for cross‑border transfer of personal data published by the PCPD (RMCs) with the overseas recipient prior to conducting any overseas transfers activities.

On 13 December 2023, the Standard Contract for the Cross-boundary Flow of Personal Information within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong) (GBA) (GBA Standard Contract) and the implementation guidelines were

announced to promote the safe and orderly cross-boundary flow of personal data within the GBA. Adoption of GBA Standard Contract is on a voluntary basis. The PCPD published guidance in December 2023 to help organizations in Hong Kong understand the applicability of the GBA Standard Contract and its relationship with the RMCs.

SECURITY

Data users are required by the Ordinance to take all practical steps to ensure that personal data is protected against unauthorized or accidental access, processing, erasure, loss or use, having regard to factors including the nature of the personal data and the harm that could result if data breaches or leaks were to occur.

Where the data user engages a data processor to process personal data on its behalf, the data user must use contractual or other means to:

- prevent unauthorized or accidental access, processing, erasure, or loss of use of the personal data; and
- ensure that the data processor does not retain the personal data for longer than necessary.

The January 2020 Consultation Paper proposed to require organizations to formulate and publish a clear data retention policy specifying retention period(s) for personal data collected. The PCPD’s Report issued in February 2023 also referred to this as an amendment direction.

BREACH NOTIFICATION

There is no statutory definition of a data breach under the Ordinance. However, under the non–binding guidance issued by the PCPD, data breach is defined as a “*suspected breach of data security of personal data held by a data user, exposing the data to the risk of unauthorized or accidental access, processing, erasure, loss or use*.”

Currently there is no mandatory requirement under the Ordinance for data users to notify authorities or data subjects about data breaches in Hong Kong. However, according to non‑binding guidance issued by the PCPD (last updated in June 2023), as a matter of best practice the PCPD encourages notification to the PCPD and to the affected data subjects as soon as practicable after becoming aware of the data breach, particularly if the data breach is likely to result in a real risk of harm to affected data subjects. Specifically, the non‑binding guidance recommends that organizations should follow the following key steps in order when handling a data breach:

- immediate gathering of essential information;
- containing the data breach;
- assessing the risk of harm;
- considering giving data breach notifications; and
- documenting the breach.

To assist organizations in reporting data breach incidents to the PCPD more effectively and in a more convenient manner, the PCPD provides an e-Data Breach Notification Form on its website.

Past high profile data incidents in recent years have led regulators and politicians to consider introducing more stringent breach notification rules. The PCPD has already hinted at increased use of compliance checks and greater publication of investigation reports as part of "fair" enforcement of the law. The January 2020 Consultation Paper proposed mandatory breach notification requirement for organizations to notify a data incident to both the PCPD and the impacted data subjects within the prescribed period where there is a real risk of significant harm. The PCPD’s Report issued in February 2023 also indicated that establishing a mandatory data breach notification mechanism would be one of the upcoming amendments.

ENFORCEMENT

The PCPD is responsible for enforcing the Ordinance. Generally, unless a specific offense applies, if a data user is found to have contravened the data protection principles of the Ordinance, the PCPD may issue an enforcement notice requiring the data user to take steps to rectify the contravention. Failure to abide by the enforcement notice is a criminal offense, punishable by a fine of up to HK$ 50,000 and imprisonment for up to two years, as well as a daily penalty of HK$ 1,000 if the offense continues after

conviction. In the case of subsequent convictions, additional and more severe penalties apply. There are also certain specific offenses under the Ordinance which are triggered directly without the intermediary step of an enforcement notice. For example:

- breach of certain provisions relating to direct marketing is punishable by a fine of up to HK$1 million and imprisonment of up to five years, depending on the nature of the breach; and
- disclosing personal data of a data subject obtained from a data user without the data user's consent is an offense punishable by a fine of up to HK$1 million and imprisonment of up to five years, where such disclosure is made with certain intent, or where the disclosure causes psychological harm to the data subject.

Appeals from enforcement decisions of the PCPD may be made to the Administrative Appeals Board.

In addition to criminal sanctions, a data subject who suffers damage by reason of contravention of the Ordinance may also seek compensation from the data user through civil proceedings. The PCPD operates an assistance scheme for data subjects in this regard.

In light of high profile data incidents in recent years, the PCPD may further strengthen its enforcement against breaches of the Ordinance through more frequent compliance checks and publication of investigation reports, as well as increased co‑ operation with local and international authorities.

The January 2020 Consultation Paper proposed to confer additional powers on the PCPD to impose administrative fines linked to the annual turnover of the organization, which would, if implemented, result in a significant increase in financial penalties at a much higher amount calculated by reference to annual turnover. The PCPD’s Report issued in February 2023 also mentioned empowering the PCPD to impose administrative fines linked to annual turnover as an amendment direction.

Doxxing

Under the Amendment Ordinance it is an offence to disclose, without the data subject’s consent, any personal data with an intent to cause harm to the data subject or any family member of the data subject.

Depending on the severity of the offence, any person who commits the offence is punishable on conviction with:

- a fine at level 6 (i.e. HK$100,000) and to imprisonment for 2 years; or
- a fine of HK$1,000,000 and to imprisonment for 5 years if the disclosure causes harm to the data subject or any family member of the data subject.

The PCPD is also empowered to conduct criminal investigations and commence prosecution for doxxing offences. Among other things:

- The PCPD is granted wide powers under the Amendment Ordinance to access documents and information from any person, or require any person to answer questions or provide relevant materials to facilitate an investigation in relation to doxxing offences.
- The PCPD may also, with a warrant, enter premises and seize any materials or devices in the premises which may be relevant to the investigation as well as decrypt any material stored in these devices.

As the anti‑doxxing provisions have extra‑territorial effect, the PCPD is empowered to serve cessation notices to operators of electronic platforms including websites and online applications (regardless of whether these operators are based in Hong Kong or outside Hong Kong) where personal data has been disclosed without the individual's consent. The cessation notices will require the recipient of the notice to take steps to remove the doxxing content or restrict the disclosure of personal data which has been made.

Failure to comply with the cessation notice is an offence. Persons contravening the offence will be liable, on first conviction, to a fine at level 5 (i.e. at HK$ 50,000) and to imprisonment for two years.

Since the Amendment Ordinance came into force to the end of 31 October 2023, the PCPD commenced 228 criminal investigations and arrested 40 persons in 39 cases among which 13 persons were charged with doxing offences and 11 of them being convicted. The longest imprisonment sentence was eight months. The PCPD also referred 55 cases to the Hong Kong

Police Force in respect of the more serious cases and cases involving other criminal offences. In addition, the PCPD issued over 1,800 cessation notices to 41 online platforms, requesting the removal of nearly 27,000 doxxing messages with a compliance rate of over 95% and over 180 doxxing channels being removed.

ELECTRONIC MARKETING

Specific provisions of the Ordinance govern the use and sharing of personal data for the purposes of direct marketing (meaning the offering, or advertising the availability of goods, facilities or services, or the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes), when such marketing is conducted through "direct marketing means" (being the sending of information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication; or making telephone calls to specific persons).

The direct marketing provisions generally require data users who wish to use personal data for the data user's own direct marketing purposes to obtain prior consent from the data subject for such action and notify the data subject as follows:

- that the data user intends to use the individual's personal data for direct marketing;
- that the data user may not so use the personal data unless the data subject has received the data subject's consent to the intended use;
- the kind(s) of personal data to be used;
- the class(es) of marketing subjects (i.e. goods / services to be marketed) in relation to which the data is to be used; and
- the response channel through which the individual may, without charge, communicate the individual's consent to the intended use.

Furthermore, if the consent was given orally, data users have the additional obligation to send a written confirmation to the data subject confirming the particulars of the consent received.

The direct marketing provisions generally require data users who wish to share personal data with a group company or a third party for direct marketing purposes (e.g. for joint marketing, or in connection with a sale of a marketing list) to obtain their prior written consent and to notify the data subject as follows:

- that the data user intends to provide the individual's personal data to another person for use by that person in direct marketing;
- that the data user may not so provide the data unless the data user has received the individual's written consent to the intended provision;
- that the provision of the personal data is for gain (if it is to be so provided);
- the kind(s) of personal data to be provided;
- the class(es) of persons to which the data is to be provided;
- the class(es) of marketing subjects (i.e. goods / services to be marketed) in relation to which the data is to be used; and
- the response channel through which the individual may, without charge, communicate the individual's consent to the intended use.

When data users use personal data for the purposes of direct marketing for the first time, they must inform the subjects that they may opt out at any time, free of charge. In practice, it is common for subsequent direct marketing communications in Hong Kong to contain unsubscribe functions, not just in the first message.

Hong Kong's anti–spam framework is set out in the Unsolicited Electronic Messages Ordinance (Cap. 593), under which three types of Do–Not–Call (DNC) registers are maintained, namely the DNC for fax, short messages and pre–recorded telephone messages. Person-to-person telemarketing calls are not regulated by this framework.

In 2019, a legislative proposal was published to implement the new DNC to provide an "opt out" framework to permit recipients to request to stop receiving person‑to‑person telemarketing calls. At the time of writing, the relevant bill is not yet announced.

ONLINE PRIVACY

The principles as stated in the Ordinance also apply in the online environment. For example, under the Ordinance, data users have the obligation to inform data subjects of the purposes for collecting their personal data, even if personal data is collected through the Internet. If a website uses cookies to collect personal data from its visitors, this should be made known to them. Data users should also inform the visitors whether and how non‑acceptance of the cookies will affect the functionality of the website.

With the coming into effect of the Amendment Ordinance, anti‑doxxing law is now in force in Hong Kong. It is an offence to disclose any personal data without the data subject's consent with an intent to cause harm to the data subject or any family member of the data subject.

KEY CONTACTS

Carolyn Bigg
Partner, Global Co-Chair of Data Protection, Privacy and Security Group
T +852 2103 0576
carolyn.bigg@dlapiper.com

Venus Cheung
Registered Foreign Lawyer
T +852 2103 0572
venus.cheung@dlapiper.com

Angele Lok
Associate
T +852 2103 0677
angele.lok@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

HUNGARY

Last modified 11 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Hungarian Parliament implemented the GDPR into Hungarian laws by amending Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information. As of 26 April 2019 all the relevant sectorial laws were also amended in Hungary in order to comply with the provisions of the GDPR.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor " *processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Hungarian Supervisory Authority is the Hungarian National Authority for Data Protection and Freedom of Information (in Hungarian: *Nemzeti Adatvédelmi és Információszabadság Hatóság*).

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain

comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to

requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, Oriental Republic of Uruguay, New Zealand, the Republic of Korea, the United Kingdom (which also covers data exchanges in the law enforcement sector which are governed by the Law Enforcement Directive – Article 36 of Directive (EU) 2016/680), and the United States of America (commercial organisations participating in the EU-US Data Privacy Framework).

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses and derogations. On 16 July 2020 the Court of Justice of the European Union (CJEU) in its *Schrems II* decision invalidated the EU-US Privacy Shield Framework, and created new obligations, notably for businesses transferring personal data pursuant to standard contractual clauses. On 10 July 2023, the European Commission adopted its long-awaited adequacy decision for the EU-US Data Privacy Framework (DPF). The new adequacy decision allows personal data to flow from the European Economic Area to DPF-certified US companies without the need for additional data protection safeguards.

The CJEU in its Schrems II decision affirmed that the protections of EU law for personal data must follow the data when transferred outside the EU; the protection provided in the destination country must be essentially equivalent to EU laws. The CJEU specifically tasked data exporters with assessing transfers on a case-by-case basis and putting into place supplementary measures (technical, organizational and / or contractual measures) whenever necessary to ensure essentially equivalent protection.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

- explicit informed consent has been obtained;
- the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defense of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
- the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-

law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon,

the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (*eg,* an email address is likely to be ‘personal data’ for the purposes of the Act).

Also, pursuant to Act No. XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities, unless otherwise provided by specific other legislation, advertisements may be conveyed to natural persons by way of direct contact (hereinafter referred to as ‘direct marketing’), such as through electronic mail or equivalent individual communications only upon the express prior consent of the person to whom the advertisement is addressed. The request for the consent may not contain any advertisement, other than the name and description of the company.

The statement of consent may be made in any way or form, on condition that it contains the name of the person providing it, and – if the advertisement to which the consent pertains may be disseminated only to persons of a specific age – his place and date of birth, furthermore, any other personal data authorized for processing by the person providing the statement, including an indication that it was given freely and in possession of the necessary legal information.

The statement of consent may be withdrawn freely any time, free of charge and without any explanation. In this case all personal data of the person who has provided the statement must be promptly erased from the records and all advertisements must be stopped.

Pursuant to Act No. C of 2003 on Electronic Communications (‘EC Act’), applying automated calling system free of any human intervention, or any other automated device for initiating communication in respect of a subscriber for the purposes of direct marketing, providing information and market research shall be subject to the prior consent of the subscriber. Furthermore, providers of electronic communications services shall not apply automated calling system free of any human intervention, or any other automated device for initiating communication in respect of a subscriber for the purposes of public opinion polling if the user opposes it (opt-out system).

ONLINE PRIVACY

The EC Act deals with the collection of location and traffic data by public electronic communications services providers ('CSPs') and use of cookies (and similar technologies).

Traffic Data

With certain special exceptions set out in the EC Act (*eg,* invoicing, collecting subscriber fees, law enforcement, national security and defense), traffic data relating to subscribers and users processed and stored by CSPs while providing such services must be erased or made anonymous when it is no longer needed.

CSPs may use certain traffic data as referred to in the EC Act for the provision of value added services or for marketing purposes subject to the subscriber’s or user’s prior consent, to the extent necessary for the provision of such services or for marketing purposes. CSPs shall provide the possibility for users or subscribers to withdraw their consent at any time.

Location Data

CSPs shall be authorized to process location data only upon the prior consent of the subscribers or users to whom the data are related, and only to the extent and for the duration as it is necessary for the provision of value added services.

Users and subscribers shall have the right to withdraw their consent at any time.

CSPs shall be required to comply with any request for location information in connection with specific subscribers or users, if made by the investigating authority, the public prosecutor, the court or the national security service pursuant to the authorization conferred in specific other legislation, to the extent required to discharge their respective duties.

Cookie Compliance

Pursuant to the EC Act, on the electronic communication terminal equipment of a subscriber or user, information may be stored, or accessed, only upon the user’s or subscriber’s prior consent granted in possession of clear and comprehensive information, which information inter alia includes the purpose of processing.

The European Data Protection Board issued a guidance in respect of the interpretation of ‘consent’ and how this consent should be obtained in practice. This guidance shall apply to the implementation of cookies as well. General practice is that consent should be obtained by means of a cookie banner. It needs to be ensured that no cookies are set / placed prior to the declaration of consent.

KEY CONTACTS

Zoltan Kozma
Partner
T +3615101154
zoltan.kozma@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ICELAND

Last modified 11 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The GDPR was incorporated in the EEA Agreement by a Joint Committee Decision dated July 6, 2018. The Act No. 90 /2018 on Data Protection and the Processing of Personal Data (the ‘**DPA**’) implements the GDPR in Iceland. The law contains derogations and exemptions from the position under the GDPR in certain permitted areas.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor " *processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The DPA defines a public authority or body in accordance with Article 1 of the Administrative Procedures Act no. 37 /1993. The term public authority refers to all parties, institutions, committees, etc. which are governed by state and local government.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Data Protection Authority (Icelandic: ‘*Persónuvernd*’) is the supervisory authority in Iceland for the purposes of Article 51 of the GDPR.

Contact details:
Persónuvernd – The Icelandic Data Protection Authority
Rauðarárstígur 10, 105 Reykjavík, Iceland.
Tel. +354 510-9600
postur@personuvernd.is
www.personuvernd.is

The Board of Directors and employees of the Data Protection Authority have an obligation of confidentiality in accordance with Chapter X of the Icelandic Administrative Procedures Act no. 37/1993. The same applies to others who work on behalf of the Authority.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

According to Article 31 of the DPA, controllers need to consult with and obtain prior authorization from the supervisory authority in relation to processing by a controller for the performance of a task carried out in the public interest.The GDPR generally implies certain withdrawal from the previous policy that processing of personal data may be based on licenses, but this Article in the DPA is an exception. The Data Protection Authority’s Rules no. 811/2019 on processing subject to authorization provides for a list of processing activities which are subject to the Authority’s written authorization, such as the transfer of sensitive personal data, which is stored with authorities, to third parties for research purposes.

Article 30 of the DPA implements the requirement to consult the supervisory authority in certain cases following a data protection impact assessment. Furthermore advertisement no. 828/2019 lists the processing activities that require a data protection impact assessment.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

Iceland did not extend the requirement to appoint a Data Protection Officer, cv. Article 37(4) of the GDPR.

The DPA defines a public authority or body in accordance with Article 1 of the Administrative Procedures Act no. 37 /1993. The term public authority refers to all parties, institutions, committees, etc. which are governed by state and local government. According to the bill to the DPA, it is regarded desirable that companies entrusted with certain projects for the public interest designate a Data Protection Officer with regard to those projects. Such projects are for example in the field of public transport, road construction and energy utility.

The Data Protection Officer may not disclose any information brought to his or her knowledge in the course of his or her work and covered by the obligation of professional secrecy. Further, the Data Protection Officer has an obligation of confidentiality in accordance with Chapter X of the Icelandic Administrative Procedures Act no. 37/1993.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle

of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose;
- the context in which the data have been collected;
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible);
- the possible consequences of the new processing for the data subjects; and
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Criminal convictions and offences data (Article 10)

According to Article 12 of the DPA, processing of personal data relating to criminal convictions and offences is subject to certain conditions and the processing must be based on one of the legal basis in Article 9 of the DPA, cf. Article 6(1) of the GDPR.

According to Article 12(1) of the DPA, authorities may not process data relating to criminal convictions and offences unless it is necessary for the purpose of their statutory tasks.

According to Article 12(2) of the DPA, the data cannot be disclosed unless:

- the data subject has explicitly given its consent for the disclosure;
- disclosure is necessary for the legitimate interests of the public or private sector which obviously outweigh the interests of the confidentiality of the data, including the interests of the data subject; or
- the disclosure is necessary for the legitimate tasks of the relevant authority or for the authority’s decision or disclosure is necessary for public-sector projects that have been legally assigned to private parties.

Private entities cannot process information on criminal convictions and offences unless the data subject has given its explicit consent or the processing is necessary for legitimate interests which obviously outweigh the interest of the data subject.

Use of personal identification numbers

According to Article 13 of the DPA, the use of a personal identification number is authorised if its purpose is objective and necessary to ensure secure personal identification. The Data Protection Authority may prohibit or order the use of a personal identification number.

Children's consent to information society services (Article 8)

Article 8(1) of the GDPR stipulates that a child may only provide their own consent to processing in respect of information society (primarily, online) services, where that child is over 16 years of age, unless member state law applies a lower age. The DPA reduces the age of consent for these purposes to 13 years for Iceland, cf. Article 10(5).

Data subject’s rights

The data subject has the right to be informed about the processing of his personal data, however, Article 17 of the DPA implements certain restrictions from these rights.

According to Article 17(3) of the DPA, Articles 13(1)-(3), 14(1)-(4) and 15 of the GDPR regarding the data subjects’ rights do not apply if the interests of individuals linked to the personal data, including the interests of the data subject itself, outweigh the interests of the data subject.

The rights granted to the data subject in Articles 13 – 15 of the GDPR can be restricted with a legislative measure if such a limitation of fundamental rights and freedoms constitutes necessary and proportionate measure in a democratic society to safeguard:

- national security;
- national defense;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security;
- other important objectives of general public interest, in particular those of economic or financial interest including monetary, budgetary and taxation matters, public health and social security;
- the protection of the data subject, the vital interests of the public or the fundamental rights of others;
- the enforcement of civil law claims; and
- legal obligation of professional secrecy.

The right to restrict the data subjects right also applies to personal data in working documents used in preparation for the controllers’ decisions if it has not been distributed to others, to the extent necessary to ensure the preparation of the proceedings.

Information regarding cases that are being processed by authorities may be exempted from access according to Article 15 (1) of the GDPR to the same extent as applies according to the Information Act no. 140/2012 and the Administrative Procedures Act no. 37/1993.

Rules No. 50/2023 on Electronic Surveillance

Rules No. 50/2023 on Electronic Surveillance apply to electronic monitoring in public places, as well as in workplaces, schools and other areas where a limited group of people usually moves around, i.e. in the common area of apartment buildings or on a common lot. The rules apply regardless of what type of equipment is used, such as surveillance cameras, web cameras, tachographs, positioning equipment or telemonitoring equipment. The rules set out requirements for the collection, distribution and storage of data collected by means of electronic surveillance. All processing of personal data must meet the requirements of GDPR on the basis of the provisions of the rules.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defense of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

Article 16 of the DPA implements the provisions of GDPR on the transfer of personal data to third countries and international organisations into Icelandic national legislation. The same restrictions therefore apply as under the GDPR.

Furthermore advertisement no. 1155/2022 prescribes for the transfer of personal data to countries which have received an adequacy status from the European Commission.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Chapter IV of the DPA implements the provisions of the GDPR on security measures into Icelandic national legislation.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

A personal data breach is defined in the DPA as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Regarding the security of the processing and notification of a personal data breach, Articles 32, 33 and 34 of the GDPR are implemented into Icelandic national legislation via Article 27 of the DPA, without any alterations.

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Data Protection Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Data Protection Authority is not made within 72 hours, it shall be accompanied by reasons for the delay. Furthermore, the processor shall notify the controller without undue delay after becoming aware of a personal data breach.

Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The Icelandic Data Protection Authority has issued guidelines for notifications of personal data breaches which are based on the instructions of the Article 29 Working Party and all such breaches, which are subject to the notification requirement, shall be notified to the Data Protection Authority via a centralized reporting portal.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Non-compliance with the instructions of the Data Protection Authority regarding a) temporary or definitive limitation including a ban on processing, b) rectification or erasure of personal data or restriction of processing and the notification of such actions to recipients to whom the personal data have been disclosed, or c) suspension of data flows to a recipient in a third country or to an international organization, can lead to daily fines until necessary improvements have been made. Fines can amount up to ISK 200,000 (approximately 1,320 euros) for each day that passes without the Data Protection Authority’s instructions being observed.

Breaches of the DPA and the GDPR can lead to administrative fines that are imposed by the Data Protection Authority. The administrative fines may amount to ISK 100,000 (approx. EUR 660) up to 1,2 billion ISK (approx. EUR 7,900,000), or, in case of a corporation, up to 2% of its annual overall turnover globally in the previous financial year, whichever is higher, when an infringement of the provisions detailed in Article 83(4) of the GDPR has taken place.

The administrative fines may amount to ISK 100,000 to ISK 2,4 billion (approx. EUR 15,850,000) or, in case of a corporation, up to 4% of its annual overall turnover globally in the previous financial year, whichever is higher, when an infringement of the provisions detailed in Articles 83(5)-83(6) of the GDPR, cf. Article 46 of the DPA, has taken place.

Major breaches can also lead to imprisonment up to 3 years and breach of confidentiality of a data protection officer can lead to fines or imprisonment up to 1 year and in severe cases, up to 3 years, cf. Article 48 of the DPA.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon,

the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Based on the Electronic Communications Act No. 70/2022 the use of electronic communications systems, including for email and other direct marketing, is only allowed if a subscriber has given prior informed consent.

If the email address has been obtained in the context of the sale of a good or service, the controller may use it for direct marketing of the controller’s own goods or services to customers who have not objected to receiving email marketing from the controller, provided the customers are given the opportunity, free of charge, to object to such use of their email address when it is collected and each time a message is sent.

Further, all marketing emails must include the name and address of the party responsible for the marketing.

ONLINE PRIVACY

Electronic Communication Data

The Electronic Communications Act No. 70/2022 provides that any processing of electronic communication data is prohibited, including storage, listening, recording or interception, unless it takes place with the informed consent of the user or as authorized by law.

Use of any kind of systems and equipment, including software that collects and/or stores information about the user's activities or interactions in his end equipment, provides access to information stored in his end equipment or monitors his activities is prohibited except with the informed consent of the user or as authorized by law. Despite this, the use of such equipment is permitted to gain access to information and / or to technical storage for legitimate purposes and with the knowledge of the user.

Cookies are considered to fall under the definition of equipment. If the use of cookies leads to the use of IP addresses or other personal data, the processing of such data must comply with the Data Protection Act. The processing is therefore not permissible without a legal basis.

The processing of electronic communication data may only be carried out by individuals who are under the control of telecommunications companies and in charge of invoicing or managing electronic communications traffic, user inquiries, reporting misconduct, marketing electronic communications services or value-added services, and the processing shall be limited to what is necessary for the benefit of such activities.

Electronic communication data stored and processed by a telecommunication company must be erased or anonymized when it is no longer needed for transmission of an electronic communication. However, telecommunications companies must keep a minimum record of data on users’ telecommunications for six months in the interest of criminal investigations and public safety.

Location Data

Location data and IP addresses are considered personal data under the Data Protection Act.

Information on the location of equipment in public electronic communications networks or electronic communications services may only be processed if it cannot be linked to individual users or with their informed consent. This does not apply to entities that provide emergency services and are officially recognized as such.

KEY CONTACTS

LOGOS Legal Services
www.logoslegalservices.com

Hjördís Halldórsdóttir
Attorney at Law, Partner
LOGOS
T +354 540 0300
hjordis@logos.is

Áslaug Björgvinsdóttir
Attorney at Law, Partner
LOGOS
T +354 540 0300
aslaug@logos.is

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

INDIA

Last modified 9 January 2024

LAW

Until recently, India did not have a standalone law or framework to govern data protection. The Information Technology Act, 2000 (**IT Act**) and rules notified thereunder formed the basis around which the data protection framework revolved. This included the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**Privacy Rules**).

In 2017, a constitutional bench of nine judges of the Supreme Court of India in *Justice K. S. Puttaswamy (Retd.) v. Union of India* [Writ Petition No. 494/ 2012] upheld that privacy is a fundamental right, which is entrenched in Article 21 [Right to Life & Liberty] of the Constitution of India. This led to the process of formulation of a comprehensive data protection framework for India. After releasing different draft versions of a data protection legislation and considering the recommendations from different stakeholders, the Ministry of Electronics and Information Technology (**MeitY**), Government of India, released the draft of the Digital Personal Data Protection Bill in 2022 (**DPDP Bill**).

The version of the DPDP Bill which was eventually passed by both houses of the Indian Parliament marked a few significant changes to the original draft of the DPDP Bill. On August 11, 2023, the Government of India published that version as the Digital Personal Data Protection Act, 2023 (**DPDP Act**), which is now part of the personal data protection and regulatory regime in India. The DPDP Act introduces several compliances with respect to the collection, processing, storage and transfer of digital personal data. However, further actions on behalf of the Government may be required to make the DPDP Act effective, including notifying the rules and regulations required for effective implementation and enforcement of the DPDP Act. The DPDP Act is applicable only to personal data in digital form and does not regulate non-personal and non-digital data. Considering this, collection and handling of non-personal data is currently unregulated in India.

Note

The DPDP Act has been drafted on the following principles:

- usage of personal data by an organization is to be done in a manner that is lawful, fair and transparent to the individuals concerned;
- usage of personal data is to be limited to the purpose for which it was collected;
- only those items of personal data that are required for attaining a specific purpose are to be collected;
- reasonable efforts should be made to ensure that the personal data of the individual is accurate and kept up to date;
- storage of data is required to be limited to such duration as is necessary for the stated purpose for which personal data was collected;
- reasonable safeguards are to be undertaken to ensure that there is no unauthorised collection or processing of personal data. This is intended to prevent personal data breach; and
- the person who decides the purpose and means of processing of personal data i.e. Data Fiduciary is accountable for such processing.

Scope and Applicability

The DPDP Act pertains to the processing of digital personal data within India, encompassing situations where the personal data is either (i) collected in a digital form or (ii) collected in a non-digitized form and subsequently converted into digital form. Consequently, the DPDP Act does not apply to the processing of personal data in its non-digitized state. The DPDP Act defines ‘personal data’ broadly to include any data about an individual who is identifiable by or in relation to such data. It also defines ‘digital personal data’ as personal data in digital form.

While the DPDP Act is applicable to Indian entities which engage in the processing of personal data, it also has extra-territorial applicability, applying to foreign entities who offer goods and services to Data Principals (as defined below) located within the territory of India and process personal data in connection to such activities. The DPDP Act does not apply to (i) personal data utilized by an individual for personal or domestic purposes or (ii) personal data deliberately made publicly accessible by either the Data Principal to whom the personal data relates or any other individual or entity mandated by law to disclose personal data to the public.

DEFINITIONS

Definition of personal data

Under the DPDP Act, Personal Data refers to data about an individual who is identifiable either by such data or in relation to such data. This implies that anonymized data or non-personal data will not be covered by the DPDP Act.

The DPDP Act also defines ‘Data Fiduciary’, ‘Data Processor’ and ‘Data Principal’, among other concepts:

Definition of Data Fiduciary

Similar to ‘Controller’ as defined under the European Union's General Data Protection Regulation (**EU-GDPR**), the DPDP Act defines Data Fiduciary as an individual or entity that, either independently or in conjunction with others, determines the purpose and means of processing of personal data.

Definition of Data Processor

Data Processor is defined as any person who processes personal data on behalf of a Data Fiduciary.

Definition of Data Principal

Similar to ‘Data Subject’ under the EU-GDPR, the DPDP Act defines Data Principal as individual to whom the personal data relates. When dealing with personal data of a child under the age of eighteen years, the term Data Principal encompasses the child's parents or legal guardian. Likewise, for persons with disabilities, it includes their legal guardian, who acts on their behalf. The DPDP Act seeks to only protect personal data of natural persons and does not include data of companies.

Definition of Processing

The DPDP Act defines ‘processing’ to mean a “*wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.*” This definition closely aligns with the concept of ‘processing’ as defined under the EU-GDPR. Nevertheless, it is important to note that while the EU-GDPR's definition encompasses both automated and specific non-automated processes, the DPDP Act confines the scope of processing solely to ‘automated’ operations.

NATIONAL DATA PROTECTION AUTHORITY

Data Protection Board of India

The DPDP Act provides for the establishment of a Data Protection Board of India (**Board**), an independent body tasked with overseeing the implementation and enforcement of the DPDP Act. The Government of India is yet to establish the Board. The Board has been envisaged as an online complaint resolution mechanism, with all its proceedings being conducted online. Once established, the Board will conduct inquiries based on complaints, address personal data breaches, and issue directions and impose penalties for non-compliance. The Board is required to scrutinize the contravention, conduct an inquiry, and communicate its decision in writing. An appeal against any order of the Board will lie with the Telecom Disputes Settlement and Appellate Tribunal (TDSAT). Other civil courts are restricted from entertaining any suit or proceeding in respect of any matter for which the Board is empowered under the DPDP Act. Thereafter, a final appeal may be made to the Supreme Court of India. Hence, a three-tier appeal mechanism has been established under this regime.

REGISTRATION

There is no registration requirement for Data Fiduciaries under the DPDP Act. However, Consent Managers are required to register themselves with the Board.

Consent Managers

The DPDP Act provides for Consent Managers registered with the Board and defines them as a single point of contact to enable a Data Principal to give, manage, review and withdraw their consent through an accessible, transparent and interoperable platform. A Data Principal may give, manage, review or withdraw their consent through a Consent Manager. Consent Managers are accountable to the Data Principal and act on behalf of the Data Principal in such manner and subject to obligations as may be prescribed. However, it is yet to be prescribed if all Data Fiduciaries are expected to integrate with the Consent Managers for seeking consent of the Data Principals and the way the Consent Manager is required to perform its functions. Additionally, the Board may impose penalties on Consent Managers, in respect of breach in observance of its obligations in relation to Data Principal’s personal data, or breach of any condition of registration of the Consent Manager.

DATA PROTECTION OFFICERS

Under the DPDP Act, Data Fiduciaries are required to appoint a contact person to address any questions that a Data Principal may have about the processing of their personal data. Significant Data Fiduciaries are required to appoint a Data Protection Officer for the same purpose. The Data Protection Officer is required to be based in India and will be responsible to the board of directors or any similar governing body of the Data Fiduciary. The Data Protection Officer will also be the point of contact for a Data Principal for the purpose of grievance redressal under the DPDP Act.

COLLECTION & PROCESSING

Legal Basis for Processing Personal Data

Under the DPDP Act, a Data Fiduciary can only process personal data for a lawful purpose and, barring limited exceptions as prescribed, is required to do so either on the basis of consent of a Data Principal or for certain ‘legitimate uses.’

Consent and Notice

The DPDP Act requires Data Fiduciaries to provide notice and obtain consent from Data Principals on or before processing personal data. At the time of collecting the consent, a notice is required to be given to the Data Principal, conveying the following information:

- the personal data intended for processing and the purpose for such processing;
- the manner in which Data Principals can exercise their rights under the DPDP Act;
- the manner for filing a complaint with the Board; and
- the contact details of the Data Protection Officer or any other person responsible for responding to a Data Principal’s requests to exercise their rights under the DPDP Act.

Data Fiduciaries are required to give an option to Data Principals to access the request for consent and the notice in English or any of the twenty-two (22) languages specified in the Eighth Schedule to the Constitution of India. The Government of India will prescribe the manner and form of the notice in subsequent legislations.

Under the DPDP Act, Data Fiduciaries may process personal data based on consent from Data Principals which is required to be:

- free, specific, informed, unconditional, and unambiguous;
- provided through clear affirmative action; and
- limited to the personal data that is necessary for the specified purpose.

Where a Data Principal has given consent to processing of their personal data prior to the commencement of the DPDP Act, the Data Fiduciary is required to provide notice containing the above details “as soon as it is reasonably practicable”. The express timeline is yet to be prescribed.

Legitimate Uses

The DPDP Act permits the processing of personal data for certain legitimate uses and in such cases, Data Fiduciaries are not required to provide prior or post-facto notice to or obtain consent from the Data Principals. The legitimate uses are as follows:

- where a Data Principal voluntarily provides their personal data to a Data Fiduciary and has not indicated to the Data Fiduciary that they do not consent to the use of their personal data;
- for the State or any of its instrumentalities to provide or issue benefits or services to Data Principals where:
    - the Data Principals have previously consented to the processing of their personal data for availing any benefits or services from the State or any of its instrumentalities; or
    - such personal data is available in digital form or in non-digital form and digitized subsequently from any database, register, book or other document maintained by the State or any of its instrumentalities;
- for the performance of any function by the State or any of its instrumentalities under any law currently in force in India or in the interest of sovereignty and integrity of India or security of the State;
- for compliance with any judgment or order issued under the law in force in India, or any judgement or order relating to contractual claims of a civil nature under any law in force outside India;
- responding to a medical emergency involving threat to life or immediate threat to health;
- for taking measures to ensure safety of, or provide assistance or services to, any individual during disaster, or any breakdown of public order; and
- for purposes relating to employment or those related to safeguarding the employer from loss or liability.

Retention of Personal Data

Data Fiduciaries are required to cease to retain personal data as soon as:

- it is reasonable to assume that the purpose for which personal data was collected is no longer being served;
- the Data Principal withdraws their consent; or
- upon a request for erasure by the Data Principal, unless retention of personal data is necessary under any other laws.

Processing of Personal Data of Certain Classes of Individuals

The DPDP Act imposes additional obligations and responsibilities on Data Fiduciaries when they are processing the personal data of children and individuals with guardians. Data Fiduciaries, before processing the personal data of children or persons with disabilities, are required to obtain verifiable consent from a parent or legal guardian, as may be applicable. However, the procedure for obtaining such verifiable consent is yet to be prescribed.

While the DPDP Act explicitly defines a child as an individual below the age of eighteen years, it does not provide a definition for ‘a person with a disability.’ However, reference may be made to the Rights of Persons with Disabilities Act, 2016 wherein this term is defined.

Specifically for children’s data, a Data Fiduciary is required to refrain from:

- undertaking any processing that is likely to have a detrimental effect on the well-being of a child; and
- tracking, monitoring the behaviour of, or directing targeted advertisements at children.

These obligations related to children’s data may be exempted by the Government under certain circumstances for prescribed purposes, class of Data Fiduciaries and for certain prescribed ages (further detailed in the section on Exemptions).

With respect to the processing of an employee’s personal data, the DPDP Act considers it as a legitimate use wherein an employer will not have to obtain express consent in order to process personal data as long as the processing is carried out for employment purposes, or to protect employers from loss or liability, or to provide a benefit to an employee.

Obligations of Data Fiduciaries

The DPDP Act prescribes certain obligations on Data Fiduciaries in collecting and processing personal data:

- complying with the DPDP Act in respect of any processing undertaken by a Data Fiduciary or on their behalf by a Data Processor, irrespective of any agreement to the contrary or failure of the Data Principal to carry out their duties provided under the DPDP Act;
- engaging a Data Processor to process personal data on its behalf only under a valid contract;
- implementing appropriate technical and organizational measures to ensure effective adherence with the provisions of the DPDP Act and any rules which may be notified;
- ensuring accuracy, completeness and consistency of the personal data when such personal data is processed to make a decision that affects the Data Principal or if the personal data is likely to be disclosed to another Data Fiduciary;
- protecting all personal data in its possession or under its control by taking reasonable security safeguards to prevent personal data breach;
- in the event of a personal data breach, notifying the Board and each affected Data Principal;
- publishing the business contact information of the Data Protection Officer in the case of Significant Data Fiduciary, or the contact person who is able to answer Data Principals’ questions regarding processing of their personal data;
- subject to compliance with other laws, deleting personal data by itself and ensuring such deletion by the Data Processor (if applicable), either when the Data Principal withdraws their consent or when it is reasonably assumed that the specified purpose is no longer being served, whichever is earlier; and
- establishing an effective grievance redressal mechanism to redress Data Principals’ grievances.

Obligations of Significant Data Fiduciaries

The Government of India may classify a Data Fiduciary, or a class of Data Fiduciaries as a Significant Data Fiduciary (SDF) based on certain factors like the volume and sensitivity of personal data processed, the risk posed to the rights of a Data Principal, the potential impact on the sovereignty and integrity of India, the risk to electoral democracy, security of the State, and public order. Upon getting notified as an SDF, entities are required to follow additional obligations:

- to designate a Data Protection Officer situated in India to serve as the SDF’s representative for compliance with the DPDP Act and the primary point of contact for addressing grievances. The appointed person should be an individual responsible to the board of directors or a similar governing body of the SDFs.
- to appoint an independent data auditor to assess the SDF's compliance with the DPDP Act. The subordinate legislations under the DPDP Act will specify the periodicity for conducting such audits, and the technical and operational qualifying criteria for auditors.
- to undertake Data Protection Impact Assessments, periodic audits, and other measures that will be prescribed by the Government of India.

Rights and Duties of Data Principals

Under the DPDP Act, Data Principals have been given certain rights which include:

- **Right to access information about personal data**: A Data Principal has the right to request a Data Fiduciary for a summary of their personal data being processed and the processing activities being undertaken by the Data Fiduciary. A Data Principal also has the right to request the Data Fiduciary for the identities of other Data Fiduciaries and Data

Processors with whom their personal data is being shared and a description of the personal data being shared. The Government of India may prescribe any other information which a Data Principal has the right to request from a Data Fiduciary in subsequent legislations.

- **Right to correction of personal data**: A Data Principal has the right to request for correction of personal data that may be inaccurate or misleading, completion of personal data that is incomplete and updating of their personal data.
- **Right to erasure**: A Data Principal has the right to request for erasure of their personal data, the processing of which was previously consented to, unless retention is necessary for compliance with any laws.
- **Right to withdraw consent**: A Data Principal has the right to withdraw consent from processing of their personal data at any time after they have provided their consent to a Data Fiduciary.
- **Right of grievance redressal**: A Data Principal has the right to grievance redressal provided by a Data Fiduciary or a Consent Manager, which is exercisable in respect to a Data Fiduciary’s obligations and a Data Principal’s rights under the DPDP Act. The time period within which a Data Fiduciary or Consent Manager is required to respond to the grievances will be prescribed in subsequent legislations.
- **Right to nominate**: A Data Principal has the right to nominate any other individual to exercise the rights of a Data Principal on their behalf, in the event of their death or incapacity.

The right to access information, correction and erasure will apply only in cases where the Data Principal has given consent or voluntarily provided their personal data to a Data Fiduciary for processing. These rights will not be available where personal data is being processed under the grounds of legitimate use. The manner in which these rights are to be exercised by a Data Principal will be prescribed by the Government of India.

Under the DPDP Act, certain duties have also been assigned to Data Principals, which include:

- complying with all applicable laws while exercising their rights under the DPDP Act;
- prohibition of impersonation of others while providing their personal data for a specified purpose;
- not suppressing any material information while providing their personal data for any document, unique identifier, proof of identity or proof of address issued by the State or any of its instrumentalities;
- not registering false or frivolous grievances or complaints with a Data Fiduciary or the Board; and
- furnishing information that is verifiably authentic while exercising the right to correction or erasure.

TRANSFER

Under the DPDP Act, transfer of personal data for the purpose of processing is permitted to any country or territory outside India, except to countries which have been specifically blacklisted by the Government of India. The list of countries to which cross-border data transfers are not permitted will be notified by the Government of India. Further, Data Fiduciaries may transfer personal data to another Data Fiduciary or Data Processor only under a valid contract.

While the DPDP Act does not provide any guidelines or requirements with respect to the contract regulating the data transfer, such data transfer agreements may contain adequate indemnity provisions for a third-party breach and may specify a mode of transfer that is adequately secured and safe. Additionally, the DPDP Act provides for certain indirect obligations on Data Processors which may be incorporated in the data transfer agreements. These include:

- implementing reasonable security safeguards to prevent personal data breach;
- reporting of personal data breaches to the Data Fiduciary;
- erasing personal data upon receiving a communication to that effect by the Data Fiduciary; and
- restricting transfer of personal data to countries which have been blacklisted by the Government of India.

Data Localisation

While the DPDP Act itself does not provide for data localisation requirements, it recognizes that other sector-specific statutes and regulations may have restrictions on storing certain classes of data, which may include personal data.

India’s central bank, the Reserve Bank of India (**RBI**) has made it mandatory from October 15, 2018, for all payment system providers and their service providers, intermediaries, third party vendors and other entities in the payment ecosystem to ensure that all data relating to payment systems operated by them are stored in a system only in India. Interestingly, by virtue of

this regulation, RBI is seeking storage of all payment system data in India, which includes the entire payment processing cycle from request to final payout, such as customer data (name, mobile number, Aadhaar number, PAN number, etc.), payment sensitive data (customer and beneficiary account details), payment credentials (OTP, PIN, passwords, etc.), and transaction data (originating and destination information, transaction reference, timestamp, amount, etc.). However, for cross border transactions which consist of both foreign and domestic components, data pertaining to the foreign leg may be stored outside India. While data pertaining to the domestic leg should be stored in India, a copy may be stored abroad.

The Securities Exchange Board of India (**SEBI**) has issued an advisory for financial sector organizations such as merchant bankers, credit rating agencies, STP service providers, debenture trustee, depositary participants and other financial institutions which are availing the Software as a Service (SaaS) based solution for managing their governance, risk and compliance functions. This advisory also lists certain critical data sets such as credit and liquidity risk data, market risk data, system and sub-system information, supplier information, system configuration data, audit / internal audit data, network topography and design, which must be stored in India. More recently, the SEBI has issued a Framework for Adoption of Cloud Services by regulated entities. If the regulated entities are engaging cloud service providers to conduct their business functions and any data pertaining to the regulated entities is on the cloud in any form, it is required to be stored within the legal boundaries of India. However, if the regulated entity has a foreign parent entity, the original data is required to be available and readily accessible in India. This implies that a copy of such data which is on the cloud may be stored abroad.

Separately, the Insurance Regulatory and Department Authority of India (Maintenance of Insurance Records) Regulations, 2015, require insurance providers to store data related to policies and claim records of insurers on systems in India (even if this data is held in an electronic form).

Additionally, while Section 128 of the Companies Act, 2013, requires every company to prepare and store, at its registered office, books of account, other relevant books and papers and financial statements for every financial year, on August 5, 2022, the Ministry of Corporate Affairs amended this rule whereby all such relevant books and papers maintained in an electronic mode are required to remain accessible in India, at all times.

Further, the Indian Computer Emergency Response Team (**Cert-In**), issued directions on information security practices, procedure, prevention, response and reporting of cyber incidents (Cyber Security Directions) dated April 28, 2022 (in force since June 28, 2022), and the frequently asked questions released on the Cyber Security Directions, require service providers offering services to users in the country to enable and maintain logs and records of financial transactions within India.

SECURITY

Under the DPDP Act, Data Fiduciaries are required to protect the personal data under their control, with respect to any processing undertaken by them or on their behalf by a Data Processor, by taking reasonable security safeguards to prevent any kind of personal data breach. Notably, the highest quantum of financial penalty prescribed under the DPDP Act, being INR 250 Crores, is for failure on the part of a Data Fiduciary to take reasonable security safeguards to prevent personal data breach. Under the DPDP Act, there are no such prescribed standards or codes of best practices regarding security practices that have been recommended or mandated by the Government of India. It is possible that these standards and codes of best practice will be prescribed in due course.

In the absence of any guidance under the DPDP Act, the reasonable security practices and procedures may comply with the IS/ISO /IEC 27001 standard.

Data Protection Impact Assessment

Under the DPDP Act, Significant Data Fiduciaries are required to appoint an independent data auditor who will undertake periodic Data Protection Impact Assessments, which has been described as a process comprising a description of the rights of Data Principals and the purpose of processing their personal data. It also includes an assessment and management of the risks to the rights of Data Principals. The Government of India will elaborate on the process of conducting Data Protection Impact Assessments in subsequent legislations.

BREACH NOTIFICATION

Under the DPDP Act, in the event of a personal data breach, Data Fiduciary is required to inform each affected Data Principal and the Board. The specific format and method of reporting is yet to be prescribed. Personal data breach is broadly defined under DPDP Act as any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, that compromises the confidentiality, integrity, or availability of personal data. Therefore, Data Fiduciaries are required to report all types of personal data breaches, regardless of the sensitivity of the breach or its impact on the Data Principal. Under the DPDP Act, neither materiality thresholds nor express timelines have been prescribed for the reporting requirement.

The DPDP Act is not the sole regulation imposing reporting requirement for data breaches. The existing cybersecurity framework also mandates reporting of cybersecurity incidents, which may include personal data breaches, to the Cert-In. In the absence of any conflicting information, both sets of regulations will be applicable.

The Government of India has established and authorized the Cert-In to collect, analyze and disseminate information on cyber incidents, provide forecasts and alerts of cybersecurity incidents, provide emergency measures for handling cybersecurity incidents and coordinate cyber incident response activities. The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (Cert-In Rules) along with the Cyber Security Directions impose mandatory notification requirements on service providers, intermediaries, data centers and corporate entities, upon the occurrence of certain cybersecurity incidents.

Cyber security incidents have been defined to mean any real or suspected adverse events, in relation to cybersecurity, that violate any explicitly or implicitly applicable security policy, resulting in:

- unauthorized access, denial or disruption of service;
- unauthorized use of a computer resource for processing or storage of information;
- changes to data or information without authorization.

Under the Cyber Security Directions, the occurrence of the following types of cybersecurity incidents are to be reported:

- targeted scanning / probing of critical networks / systems;
- compromise of critical systems / information;
- unauthorized access of IT systems / data;
- defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code, links to external websites, etc;
- malicious code attacks such as spreading virus / worm / trojan / bots / spyware / ransomware / cryptominers;
- attack on servers such as databased, Mail and DNS and network devices such as routers;
- identity theft, spoofing and phishing attacks;
- denial of service and distributed denial of service attacks;
- attacks on critical infrastructure, SCADA and operation technology systems and wireless networks;
- attacks on applications such as e-governance, e-commerce, etc;
- data breach;
- data leak;
- attacks on internet of things devices and associated systems, networks, software and servers;
- attacks or incident affects digital payment systems;
- attacks through malicious mobile applications;
- fake mobile applications;
- unauthorized access to social media accounts;
- attacks or malicious / suspicious activities affecting cloud computing systems / servers / software / applications;
- attacks or malicious / suspicious activities affecting systems / servers / networks / software / applications related to Big Data, block chain, virtual assets, virtual asset exchanges, custodian wallets, robotics, 3D and 4D printing, additive manufacturing, drones;
- attacks or malicious / suspicious activities affecting systems / servers / software / applications related to artificial intelligence and machine learning.

These incidents can be reported to Cert-In via (i) email (incident@cert-in.org.in), (ii) phone (1800-11-4949), or (iii) fax (1800-11-6969). The reporting methods and formats are available at www.cert-in.org.in and will be updated from time to time. The compliance obligations under the Cyber Security Directions extend to all entities which have computer systems, networks and / or resources in India, irrespective of whether the entity is incorporated in or outside India.

Data Fiduciaries may review their data breach reporting protocols and assess each incident in accordance with the guidelines outlined in the DPDP Act and the Cert-In Rules to ascertain whether it necessitates reporting under either or both regulatory frameworks.

ENFORCEMENT

Under the IT Act, civil penalties are prescribed. If an entity that possesses, manages or handles any sensitive personal information in a computer resource that it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures, and its negligence causes wrongful loss or wrongful gain to any person, the entity was liable for damages to the affected person(s). In the event of unlawful disclosure of personal information, the IT Act prescribes civil penalties which may extend up to INR 2,500,000 or approximately €27,455 (as at January 9, 2024).

Separately, the Cyber Security Directions have introduced penalty of a term of imprisonment extendable to 1 year or a fine up to INR 10,000,000 or approximately €109,822 (as at January 9, 2024), or both, for failure to provide information to Cert-In or non-compliance with the Cyber Security Directions.

Under the DPDP Act, civil monetary penalties on Data Fiduciaries ranging from INR 50,000,000 or approximately € 5,498,135 to INR 2,500,000,000 or approximately €27,490,675 (as at January 9, 2024) have been prescribed for different contraventions. The DPDP Act also provides for a penalty of up to INR 10,000 or approximately €110 (as at January 9, 2024) for the contravention of duties by a Data Principal. The quantum of monetary penalty will be determined by the Board, taking into consideration the following factors:

- the nature, gravity, and duration of the breach;
- the type and nature of the personal data affected by the breach;
- repetitive nature of the breach;
- whether the person, as a result of the breach, has realised a gain or avoided any loss;
- whether the person took any action to mitigate the effects and consequences of the breach, and the timeliness and effectiveness of such action;
- whether the financial penalty to be imposed is proportionate and effective, having regard to the need to secure observance of and deter breach of the provisions of this Act; and
- the likely impact of the imposition of the financial penalty on the person.

The Government of India may amend the penalties that have been prescribed under the DPDP Act by issuing a notification in the future. However, the penalties cannot be modified to exceed double of the amount that has been specified under the DPDP Act currently. Therefore, financial penalty may not be more than INR 500 Crores even after amendment by the Government of India.

Exemptions

The DPDP Act provides for exemptions from the application of certain provisions, which are available to Data Fiduciaries in certain circumstances:

a. **Exemptions for certain Data Fiduciaries or class of Data Fiduciaries, including startups**: The Government of India will issue a notification exempting certain Data Fiduciaries or class of Data Fiduciaries, including startups, from certain provisions of the DPDP Act. This notification will be based on the volume and nature of personal data processed. Such Data Fiduciaries will not be required to comply with the following obligations:
    - issuing a notice before seeking consent of a Data Principal;
    - ensuring the accuracy and completeness of personal data;
    - erasing personal data after the purpose for which it was collected is served;

- obtaining verifiable parental consent before processing children’s data and no behavioural tracking of children or targeted advertising directed at children;
- the obligations applying to SDFs; and
- providing a Data Principal with the right to information about their personal data.

b. **Exemptions where personal data is processed for certain specified uses**: The DPDP Act exempts entities from complying with the provisions pertaining to obligations of Data Fiduciaries, rights and duties of Data Principals and transfer of personal data outside India in cases where:
   - the processing of personal data is necessary for enforcement of any legal right or claim;
   - the processing of personal data is necessary to perform judicial or quasi-judicial, regulatory or supervisory functions by a court, tribunal or any other such body entrusted by the law to perform such functions;
   - the processing of personal data is necessary in the interest of prevention, investigation or prosecution for offences or contraventions of any law;
   - personal data of Data Principals who are not within the territory of India is processed by any person based in India, pursuant to a contract with any person outside the territory of India;
   - the processing of personal data is necessary for carrying out mergers, acquisitions and other such transactions between two or more companies which have been approved by a court, tribunal or any other competent authority; or
   - the processing of personal data is done in relation to debt-recovery activities.

c. **Exemptions for research and statistical purposes**: The DPDP Act will not apply to the processing of personal data which is necessary to carry out research, archiving or statistical activities, provided that the personal data is not being used to take any decision specific to a Data Principal. The Government of India will prescribe the standards in accordance with which such processing is to be carried out.

d. **Exemptions for the Government of India**: The DPDP Act will not apply to certain instrumentalities of the Government of India in the interest of sovereignty and integrity of India, security, friendly relations with foreign countries and maintenance of public order. The Government of India will notify the instrumentalities to which this exemption is available.

The Government of India may notify additional exemptions from the provisions of the DPDP Act for any Data Fiduciary or class of Data Fiduciaries in the following five years.

ELECTRONIC MARKETING

Under the DPDP Act, Data Principals have the right to withdraw their consent and restrict their personal data from being processed by an entity for specified purposes such as email marketing. Furthermore, Data Fiduciaries are required to refrain from engaging in tracking or behavioral monitoring of children, as well as from conducting targeted advertising aimed at children.

However, in a related development, the Food Safety and Standards Authority of India (FSSAI) has made it mandatory for E-commerce FBOs (Food Business Operators) to obtain a license from the Central Licensing Authority. E-commerce FBO means any Food Business Operator carrying out any of the activities under section 3(n) of Food Safety & Standards Act, 2006, through the medium of e-commerce. Interestingly, section 3(n) covers the entire food chain as it defines “food business” as any undertaking, whether for-profit or not, and whether public or private, carrying out any of the activities related to any stage of manufacture, processing, packaging, storage, transportation, distribution of food, import and includes food services, catering services, sale of food or food ingredients. Similarly, another set of legal Rules being referred as “E-commerce & the Legal Metrology (Packaged Commodities) Amendment Rules, 2017,” effective from January 1, 2018, has made it mandatory for e-commerce entities to ensure mandatory declarations about the commodity displayed on the digital and electronic network used for e-commerce transactions.

The consumer protection regime in India was recently overhauled by way of enactment of the Consumer Protection Act, 2019 (notified in July 2020) (**CPA 2019**). Under CPA 2019, sellers and service providers have the obligation to, among others, not engage in unfair trade practices including by way of misleading advertisements. Further, Consumer Protection (E-Commerce) Rules, 2020 (**E-Commerce Rules**) have been notified under the CPA to regulate e-commerce entities in India. An ‘e-commerce entity’ has been defined to mean any person who owns, operates, or manages digital or electronic facility or platform for electronic commerce, but does not include a seller offering his goods or services for sale on a marketplace e-

commerce entity. E-commerce entities are required to set up a proper grievance redressal mechanism and consumer complaints should be acknowledged by the grievance officer within a stipulated timeline. E-commerce entities are further required to, among others, provide information in relation to refund, exchange, warranty, delivery, mode of payment, fees and charges, grievance process and other relevant information on their platform. The price (total and a break-up) of goods or services should be mentioned clearly and misleading advertisements and misrepresentations are prohibited.

In June 2022, the Central Consumer Protection Authority (**CCPA**), issued Guidelines on Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 (**the Guidelines**). The Guidelines lay down the conditions for non-misleading and valid advertisements and conditions for bait advertisements. The Guidelines prohibit surrogate advertising, and also lay down conditions for advertisements targeted at children. Moreover, the Guidelines lay down the duties of manufacturers, service providers, advertisers, and advertising agencies.

In November 2023, the CCPA further issued Guidelines for Prevention and Regulation of Dark Patterns, 2023 (**Dark Pattern Guidelines**) to restrict the use of dark patterns or manipulative practices by online platforms in designing their user interface and user experience that impair user autonomy, influence decision making, and work to the detriment of users. The Dark Pattern Guidelines apply to sellers, advertisers, and all platforms that systematically offer goods and services in India. The Dark Pattern Guidelines list certain specified dark patterns that are prohibited, including practices such as false urgency, subscription trap or confirm shaming.

Further, the National Do Not Call (**NDNC**) Registry is effectively implemented by the Telecom Regulatory Authority of India (**TRAI**). TRAI has also established the Telecom Commercial Communication Customer Preference Portal, i.e. a national data base containing a list of the telephone numbers of all subscribers who have registered their preferences regarding the receipt of commercial communications. Telemarketing companies may lose their license for repeated violation of DNC norms.

ONLINE PRIVACY

There is no regulation of cookies, behavioural advertising, or location data. However, this may include personal data and it is advisable to obtain user consent, such as by using appropriate disclaimers.

The IT Act contains both civil and a criminal penalties and offences for a variety of computer crimes. Under the IT Act, if any person introduces or causes to be introduced, any computer contaminant (like viruses etc.), into any computer, computer system or computer network, they may be liable to pay damages to the affected person(s). Under the IT Act, ‘computer contaminant’ is defined as any set of computer instructions that are designed:

- to modify, destroy, record, or transmit data or programs residing within a computer, computer system or computer network, or
- by any means to usurp the normal operation of the computer, computer system or computer network.

Further, under the IT Act, any person, who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, may be subject to a prison term of up to three years and a fine up to INR 100,000 or approximately €1,098 (as at January 9, 2024).

KEY CONTACTS

J. Sagar Associates
www.jsalaw.com/

Sajai Singh
Partner
J. Sagar Associates
T +91 80 435 03627
sajai@jsalaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

INDONESIA

Last modified 2 January 2024

LAW

Specific regulations

Indonesia has adopted an overarching framework for personal data protection through the enactment of Law No. 27 of 2022 concerning Personal Data Protection ("**PDP Law**") since 17 October 2022. Data controllers, data processors and relevant parties that process personal data are given a two (2) year transition period following the enactment of the PDP Law, thus up to 17 October 2024 to conform with the PDP Law. Once the transition period elapses, all such parties must comply with all the provisions of the PDP Law and any incompliance thereto may possibly be enforced.

The PDP Law is closely aligned with international data privacy standards, and is largely modelled on the European Union’s General Data Protection Regulation ("**GDPR**").

Before the enactment of the PDP Law, there was no comprehensive law on privacy / personal data protection in Indonesia. Instead, separate legislations which are embedded in and / or spread out in a number of sector specific (e.g. financial sector), matter specific (e.g. e-commerce), and / or nature specific (e.g. personal data processed in / through electronic systems) regulations regulate the general aspects of the protection of privacy / personal data were relied upon. Examples include the Law No. 11 of 2008 regarding Electronic Information and Transactions ("**EIT Law**") as amended by Law No. 19 of 2016 regarding the Amendment of EIT Law and Law No. 1 of 2024 regarding the Second Amendment of EIT Law, Government Regulation No. 71 of 2019 regarding the Operation of Electronic Systems and Transactions ("**Reg. 71**") and its implementing regulations such as the Minister of Communications and Informatics Regulation No. 5 of 2020 regarding the Private Sector Electronic System Operator, as lastly amended by Minister of Communications and Informatics Regulation No. 10 of 2021 ("**MOCI Reg. 5/2020**"), and Minister of Communication & Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System ("**MOCI Reg. 20/2016**"). These existing rules on privacy / personal data protection in the framework of processing personal data through electronic systems will be referred to as “General Data Protection Regulations”.

Other than provisions relating to data protection under General Data Protection Regulations, examples of sector specific regulations which also include provisions relating to data protection include the following:

Telecommunications sector

Article 40 of Law No. 36 of 1999 regarding Telecommunications ("**Telecommunications Law**") as partially amended by Law No. 11 of 2020 on Job Creation which was later revoked and replaced by Law No. 6 of 2023 on the Enactment into Law of Government Regulation in Lieu of Law No. 2 of 2022 on Job Creation (generally referred to as the "**Omnibus Law**") provides that any person is prohibited from any kind of tapping of information transmitted through any kind of telecommunications network. Article 42 paragraph (1) of the Telecommunications Law stipulates that any telecommunications services operator has to keep confidential any information transmitted or received by a telecommunications service subscriber through telecommunications networks or telecommunications services provided by the relevant operator.[1]

Public information sector

Article 6 paragraph (3) point c of Law No. 14 of 2008 regarding Disclosure of Public Information ("**Public Information Law**")[2] provides that information relating to personal rights may not be disclosed by public bodies. Furthermore, Article 17 point (h) of the Public Information Law, together with other laws, prohibits the disclosure of private information of any person, particularly that which concerns family history; medical and psychological history; financial information (including assets, earnings and bank records), evaluation records concerning a person's capability / recommendation / intellectual, and / or formal and informal education records.

Banking and capital market sectors

Data privacy in the banking sector is regulated under Law No. 7 of 1992 as amended by Law No. 10 of 1998 on Banking ("**Banking Law**") and as partially amended by the Omnibus Law and Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector, including the implementing regulations. As regards the capital market sector, it is generally regulated under Law No. 8 of 1995 on Capital Market ("**Capital Market Law**”) which was partially revoked by Government Regulation In Lieu of Law No. 1 of 2017 on Access to Financial Information for Tax Purposes and amended by Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector, including the implementing regulations. The regulations mentioned above apply to both individuals and corporate data[3].

Principally, commercial banks' customer data transfer (by way of establishing a data center or a data processing outside Indonesia territory) necessitates prior approval being obtained from the Indonesian Financial Services Authority ("**FSA**")[4].

Generally, those separate sector specific legislations will principally still be valid so long they do not contradict with the PDP Law. It is anticipated that further implementing regulations will be drawn up and issued (which may or may not revoke existing legislations on the protection of privacy / personal data), and a separate institution / agency will be formed to specifically handle and undertake the organization of the protection of privacy / personal data in accordance with the PDP Law ("**PDP Agency**").

In the meantime, the first draft of Government Regulation on the Implementation of the PDP Law ("**Draft Implementing Regulation to PDP Law**") has been circulated for public comments from August 31st, 2023 until September 25th, 2023. The drafting process was targeted to be concluded at the end of 2023, however, it seems that the legislator is still in the process of identifying and analysing a total of 1,989 input to the Draft Implementing Regulation to PDP Law, as announced through a dedicated website that is accessible at pdp.id.

1: Please note that the Omnibus Law only partially amended the Telecommunications Law, thus Articles 40 and 42 of the Telecommunications Law are still valid and fully enforced.

2: Please note that Law No. 14 of 2008 regarding Disclosure of Public Information has been partially amended with Constitutional Court Judgement Number 77 / PUU-XIV / 2016, however Articles 6 and 17 of Law No. 14 of 2008 regarding Disclosure of Public Information have not been amended.

3: Please note that the Omnibus Law does not amend the Articles that governs data protection in Banking Law.

4: Please note that Article 35 paragraph (3) of the Financial Services Authority Regulation No. 11/POJK.03/2022 on the Organization of Information Technology by Commercial Banks necessitates commercial banks to obtain prior approval from the FSA in the event such commercial banks intend to establish a data center or a data processing outside Indonesia territory.

DEFINITIONS

Definition of personal data

Personal data under the General Data Protection Regulations and the PDP Law is broadly defined as any data of an individual who can be identified and / or may be identified individually or combined with other information both directly or indirectly through electronic or non-electronic systems.

Definition of sensitive personal data

Sensitive personal data under the PDP Law is referred to as "specific personal data", which would include any (i) health data and records, (ii) biometric data, (iii) genetic data, (iv) sexual life / orientation, (v) political views, (vi) criminal records, (vii) children’s data, (viii) personal financial data, and / or (ix) any other data as (may be) provided in accordance to the prevailing laws and regulations. There is however, no clear / specific differentiation between the requirements for processing of general and specific personal data, except that:

- a data controller may be obligated to carry out a data protection impact assessment when processing personal data with a high potential risk to data subjects, which includes, among others, such an event where it would process specific personal data;
- a personal data controller and processor may be obliged to appoint a data protection officer (DPO), in the event that the main activity of the personal data controller consists of processing personal data in a large scale that involves specific personal data and / or that relates to criminal acts. Further provisions may possibly be set out in subsequent implementing regulations to the PDP Law.

NATIONAL DATA PROTECTION AUTHORITY

Under the PDP Law, a separate institution / agency (the PDP Agency mentioned earlier) will be formed to specifically handle and undertake the organization of the protection of privacy / personal data, whom will be tasked, among others, to formulate policies / strategies, to supervise / monitor the implementation of the PDP Law, to enforce administrative sanctions for non-compliance with the PDP Law, and to facilitate non-court dispute settlements. A presidential regulation would be issued in respect to such a PDP Agency, while procedures to implement the authorities of the PDP Agency will be set out in a government regulation, both which as of writing are yet to be issued.

During the two (2) year transition period of the PDP Law and until such a PDP Agency is formed and operating, the Ministry of Communications and Informatics of the Republic of Indonesia ("**MOCI**") will largely still have the authority over data privacy matters that are processed through electronic systems in accordance to the General Data Protection Regulations.

However, it does not rule out the possible enforcement by:

- other relevant sector’s regulatory authority (in the event the data controller / processor is subject to a regulated sector) which may also impose certain other administrative sanctions; for example, the FSA has the authority to act as the regulator of data privacy in the capital market sector (since 31 December 2012) and with regard to banks’ customer data privacy issues (since 31 December 2013); or
- the law enforcement agency (prosecutor) if non-compliance involves a criminal offense, which may subject the accused to imprisonment and / or fines.

REGISTRATION

The PDP Law does not contain a specific obligation to register and / or notify supervisory authorities of the processing of personal data.

However, it is to be noted that there is a general registration obligation with the MOCI for any foreign and / or Indonesian party, who provides, manages, and / or trades goods and / or services through electronic systems and / or over the internet as an electronic system operator, provided that:

- it provides services in the territory of Indonesia;
- it conducts business in Indonesia; and / or
- its electronic system is used and / or offered in the territory of Indonesia.

Such a party (commonly also referred to as a "electronic system operator" or "**PSE**") would be required to make certain registration with the MOCI before its electronic system is to be used in Indonesia which will be marked by the grant of an electronic system operator registration certificate (*Surat Tanda Terdaftar Penyelenggara Sistem Elektronik* or commonly abbreviated as "**TDPSE**").

Such a registration requirement is to ensure the reliability, security and compatibility of the electronic system in processing any personal data stored in it. Certain publication of the PSE’s profile is intended to and / or will be made on a website operated by the relevant authority (MOCI) upon successful registration.

DATA PROTECTION OFFICERS

There is no requirement in Indonesia for organizations to appoint a data protection officer except in certain situations mentioned below.

The PDP Law formally establishes the position of a data protection officer (DPO) into Indonesian law, which was nonexistent under the General Data Protection Regulations.

The PDP Law only requires data controllers and data processors to mandatorily appoint a data protection officer (DPO) in the event that:

- the personal data processing is for public service purposes;
- the main operations of the data controller require large-scale, frequent and systematic monitoring of personal data; or
- the main operations of the data controller involve large-scale personal data processing of specific personal data and / or personal data related to criminal activity.

This data protection officer (DPO) shall, at the very least, carry out the functions of:

- informing and providing advice to data controllers or data processors regarding compliance with the PDP Law;
- monitoring and ensuring compliance with the PDP Law and the internal policies of a data controller or data processor;
- providing advice regarding the personal data protection impact assessment and monitoring the performance of data controllers or data processors; and
- coordinating and acting as a contact person for issues related to personal data processing.

Further conditions on DPOs will be set out in separate a government regulation, which as of writing hereof is yet to be issued.

COLLECTION & PROCESSING

Based on the PDP Law, processing of personal data includes:

1. obtainment and collection;
2. processing and analyzing;
3. storing;
4. correction and updates;
5. displaying, announcing, transferring / transmitting, distributing or disclosure / providing access to; and / or
6. deletion or removal.

With the enactment of the PDP Law, the lawfulness of processing personal data has been extended and is largely similar with the GDPR, which are currently as follows:

- **consent**: the data subject has given explicit consent to the processing of his / her personal data for one or more specific purposes as have been conveyed by the data controller to the data subject;
- **contractual obligation**: processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject upon entering into a contract;
- **legal obligation**: processing is necessary for compliance with a legal obligation to which the controller is subject to;
- **vital interest**: processing is necessary in order to protect the vital interests of the data subject ("vital interest of the data subject" relates to the survival of the data subject such as when the processing is necessary for serious medical treatment proceedings);
- **public interest**: processing is necessary for the performance of a task carried out in the public interest, public service or the exercise of official authority vested in the data controller in accordance to prevailing laws and regulations; and / or

- **legitimate interest**: processing is necessary for the purposes of other legitimate interests with due regard to the purpose, needs and balance of interest of rights of the data controller and the data subject.

The current Draft Implementing Regulation to PDP Law (version of August 31st, 2023) suggests some further guidance containing the criteria and / or restrictions in regard to each lawful basis.

The PDP Law also re-emphasizes the principles of personal data protection that are also set out in the General Data Protection Regulations, which includes:

- personal data collection is conducted in a limited and specific manner, legally valid, fairly, with the knowledge and approval of the personal data owner (transparency);
- personal data processing is conducted in accordance with its purpose;
- personal data processing is conducted by securing the rights of the personal data owner;
- personal data processing is conducted accurately, completely, not misleading, up to date, can be accounted for, and by
- taking into account to the purpose of processing of the personal data;
- personal data processing is conducted by protecting the security of personal data from loss, misuse, unauthorized access
- and disclosure, as well as the alteration or destruction of personal data;
- personal data processing is conducted by notifying the purpose of collection, processing activities, and failure of personal
- data protection;
- personal data processing is destroyed and / or deleted except if it is still in the retention period in accordance with the necessity based on the laws and regulations; and
- processing of personal data shall be carried out responsibly and shall be verifiable in a clear manner.

TRANSFER

Cross border transfers

Transfers of personal data, including transfers outside of the territory of the Republic of Indonesia would principally require an underlying basis. Cross border transfers are principally permitted provided that, the transferring data controller is able to ensure the following:

- that the country of domicile of the data controller or data processor that will receive the transfer of personal data has an equal or higher level of personal data protection than afforded under the PDP Law ("**Adequacy of Protection**");
- in the absence of Adequacy of Protection, an adequate level of binding personal data protection shall be available (" **Appropriate Safeguards**");
- in the event that neither Adequacy of Protection nor Appropriate Safeguards are present, (prior) consent shall be obtained from the data subject.

Further terms in connection hereof, is intended to be set out in a government regulation, which as of writing hereof is yet to be issued.

The current Draft Implementing Regulation to PDP Law (version of August 31st, 2023) suggests that such Adequacy of Protection assessment will be made by the PDP Agency (which as of the date hereof is yet to be formed and operating), whom consequently may issue a list of such countries that have equal / higher level of personal data protection.In practice and for the time being, the absence of a PDP Agency as well as relevant implementing regulations to the PDP Law, implies that the General Data Protection Regulations will largely still apply, which would subject a data exporter / transferor with the obligations to:

- ensure the effectiveness of supervision by the relevant governmental institutions and law enforcer. Data exporter / transferor is obliged to provide access to its electronic system and electronic data if required in the framework of supervision and law enforcement pursuant to the prevailing laws and regulations. In practice this would imply that the data exporter / transferor shall also ensure that the country in which its electronic system and electronic data is being managed, processed and / or stored, has cooperative and / or diplomatic relations with the Republic of Indonesia, to allow relevant Indonesian government institutions and / or law enforcers to obtain access to any such required electronic system and electronic data; and

- prior to such transfer, coordinate with the Directorate General for Informatics Application (*Direktorat Jenderal Aplikasi Informatika* or commonly abbreviated as "**DITJEN APTIKA**") within the MOCI. This implies the obligation of the personal data exporter / transferor to make and submit certain reports to DITJEN APTIKA.

SECURITY

The PDP Law does not provide specific technical standards or measures. It, however, does provide certain general measures to data controllers, who are obliged to protect and ensure the security of personal data that it processes, by requiring them to:

- set out and implement operational technical measures to protect personal data from any disruption in the processing of personal data that is contrary to the provisions of laws and regulations; and
- determine the appropriate level of security of the personal data by taking into account the nature and risk of personal data which must be protected in the processing of personal data.

Whilst anticipating the issuance of further implementing regulations to the PDP Law, certain fundaments to ensuring the security of personal data may be found in the General Data Protection Regulations, which sets out certain obligations to electronic system operators (PSEs) in particular. The obligations of such PSEs are regulated under Reg. 71 and MOCI Reg. 20/2016, whom amongst other things shall:

- guarantee the confidentiality of the source code of the software;
- ensure agreements on minimum service level and information security towards the information technology services being used as well as security and facility of internal communication security it implements;
- protect and ensure the privacy and personal data protection of users;
- ensure the appropriate lawful use and disclosure of the personal data;
- provide the audit records on all provision of electronic systems activities;
- have governance policies, operational work procedures, and audit mechanisms that are conducted periodically in the electronic system;
- for private sector PSEs who process and / or store personal data outside of Indonesia, must ensure the supervisory effectiveness of the Ministry or Agency and law enforcement;
- provide access to the electronic system for the purpose of supervision and law enforcement;
- provide information in the electronic system based on legitimate request from investigators for certain crimes;
- provide options to the personal data owner regarding the personal data that is processed so that the personal data can or cannot be used and / or displayed by / at third party based on the consent as long as it is related with the purpose of obtaining and collecting the personal data;
- provide access or opportunity to personal data owner to change or renew his / her personal data without disturbing the system management of the personal data, except regulated otherwise by laws and regulations;
- delete the personal data if (i) it has reached the maximum period of storing the personal data (at the shortest 5 years or based on the applicable regulations / specific sectoral regulations); or (ii) by request from the personal data owner, except regulated otherwise by the laws and regulations; and
- provide contact person that is easy to be contacted by the personal data owner in relation to his / her personal data.

An online self-assessment on the security system’s risk level and compliance is since recently also offered upon the application for an electronic system operator registration certificate (TDPSE). Although it is a self-assessment, the feature is to a certain degree mandatory, as an applicant for TDPSE may not be able to proceed in submitting its application before it fills out certain part of the online self-assessment about its security system’s risk level and compliance.

In the telecommunications sector, Article 19 paragraph (2) of Minister of Communication and Informatics Regulation No. 26/PER /M.KOMINFO/5/2007 regarding the Security and Utilization of Internet Protocol based Telecommunications Network (as amended) ("**MOCI Reg. 26/2007**") also provides that the telecommunication service provider is responsible for data storage due to its obligation to record its log file for at least 3 months.

BREACH NOTIFICATION

The PDP Law contains a general requirement for a personal data breach to be notified by the controller to both (i) the affected personal data subjects and (ii) the PDP Agency, and for more serious breaches which would disturb public services and / or significantly affect the public interest, to also be notified to the public.

Personal data breach is a wide concept, which under the PDP Law is referred to as a "personal data protection failure" and defined as any "failure in protecting a person’s personal data in terms of confidentiality, integrity, and availability of the personal data, including security breaches, whether intentional or unintentional, which lead to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed".

The PDP Law stipulates that in the event of such a personal data protection failure, the personal data controller must deliver a written notification within 72 hours.

The PDP Law provides guidelines on the required content of the written notification, which must at least include:

- a description of the personal data that was breached;
- when and how the personal data was breached; and
- the efforts undertaken by the personal data controller to mitigate the effects of the data breach and recover affected personal data.

However, during the transition period of the PDP Law and until the PDP Agency is formed and operating, data breach notifications should continue to be submitted to the MOCI and other relevant institution(s) pursuant to General Data Protection Regulations, which includes the following terms:

A. Reporting obligations to relevant authorities:

- if there is a serious system interference or failure caused by acts of a third party on its electronic system, a report shall be made immediately and at a first instance to:
    - a law enforcement official (in practice, mostly if the breach is suspected to contain matters related to cybercrimes); and
    - relevant Ministry or Agency (namely DITJEN APTIKA, and if required (often also as a matter of custom / courtesy) its specific sector’s authority.

However, there is no specific definition or elucidation provided on what "immediately" or "first instance" shall mean. In practice, typically, such an event would be reportable if there is certain loss, namely where the impact due to failure of the electronic system has legal consequence to the user, operator and other parties, both material and immaterial.

- on the content / coverage of the report, there is no specific minimum information prescribed, except that the electronic system operator / PSE (data controller / processor), shall also take the necessary measures to secure the electronic information / document under its control.

However, in practice and pursuant to the DITJEN APTIKA’s current policy, DITJEN APTIKA has made available a prescribed notification format which shall be completed with, among others, the following information:

- How the notifying party is aware of such breach;
- Description of the event;
- Period of the incident;
- Category of the disclosed personal data (general data and / or specific data);
- Estimation of the total affected individuals;
- The affected person’s status (employee, consumer, student and etc);
- Description of the interfered components of the electronic system;
- Impact to the notifying party;
- Period of recovery (for the notifying party to recover the electronic system);
- Accessibility of data protection trainings for the individuals involved in the processing of personal data of the notifying party;

- Efforts to handle and recover from the disclosure of personal data by the personal data controller;
- Efforts to prevent future issues; and
- Notification to the affected individuals

B. Notification obligations to relevant data subject:

- a notification shall be sent within 14 (calendar) days as of discovery / determination of a breach, namely upon failure to protect the secrecy of the personal data in the electronic system.

There is no further description on what would contain a "failure to protect the secrecy of the personal data". The MOCI would as a general rule consider such a failure present, in the event that other parties (with no rights to access) may identify the affected person based on the disclosed data.

- on the content / coverage of the notification, it must at the minimum provide the reason or cause of the occurrence of the failure in protecting the secrecy of personal data. No specific format is prescribed.

ENFORCEMENT

Sanctions

In Indonesia, the sanctions for breaches of data privacy are found under the relevant legislation and are essentially fines. Imprisonment may be imposed in severe instances, such as in the event of intentional infringement.

Enforcement by the PDP Agency (administrative sanctions)

Violations of certain articles in the PDP Law are subject to administrative sanctions. These administrative sanctions, which shall be imposed by the PDP Agency, are as follows:

- written warning;
- temporary suspension of personal data processing activities;
- deletion or destruction of personal data; and / or
- administrative fines.

With regard to administrative fines, the PDP Law stipulates that the maximum fine is 2% of the concerned party's annual income or revenue. Further provisions on administrative sanctions and the procedures for the imposition of administrative fines will be provided in Government Regulations.

Enforcement by the public prosecutor (criminal sanctions)

- Every person is prohibited from unlawfully obtaining or collecting personal data not belonging to themselves, and with the intention of benefiting themselves or another person which may result in the loss for the data subject. Violation of this is subject to maximum imprisonment of five (5) years and / or a maximum fine of IDR 5 billion (±USD334,000);
- Every person is prohibited from unlawfully disclosing personal data that does not belong to themselves. Violation of this is subject to maximum imprisonment of four (4) years and / or a maximum fine of IDR 4 billion (±USD267,000);
- Every person is prohibited from using personal data that does not belong to such person in a manner that contravenes the law. Violation of this is subject to maximum imprisonment of five (5) years and / or a maximum fine of IDR 5 billion (±USD334,000);
- Every person is prohibited from creating false personal data or fake personal data with the intention of benefiting themselves or other persons that may cause harm to other persons. Violation of this is subject to maximum imprisonment of six (6) years and / or a maximum fine of IDR 6 billion (±USD400,000).

Additional penalties may also be imposed in the form of confiscation of profits and / or assets obtained or proceeds from criminal acts and indemnity payment.

If the criminal act is committed by a corporate entity, the PDP Law stipulates that criminal sanctions will be imposed only in the form of criminal fines. These fines will be imposed on the management, controller, instructor, beneficial owner, and / or the corporation itself. The administrative fines for corporate entities can be up to 10 times the maximum fines for individuals.

Additional criminal sanctions that may be imposed on corporate entities, include:

- confiscation of profits and / or assets obtained or proceeds from criminal acts;
- suspension of all or part of the business of the corporation;
- permanent prohibition on certain activities;
- closure of all or part of the business premises and / or activities of the corporation;
- fulfilment of the neglected obligation;
- payment of compensation;
- revocation of licenses; and / or
- dissolution of the corporation.

Since the above provisions relate to prohibited conducts related to personal data that shall be enforced by the public prosecutor, these would already have effect since the enactment of the PDP Law.

Enforcement by the MOCI (administrative sanctions)

Considering that there is no specific data protection authority yet formed and operating (which with the recent enactment of the PDP Law is intended to be assumed by the PDP Agency), therefore, reference hereinbelow would still apply, and it is currently still the MOCI that is responsible for monitoring and regulating data protection (in the context of personal data in electronic systems).

The MOCI has the right to request data and information from the electronic system operator (data controller / processor) for the purpose of protecting personal data.

It may also enforce non-complying parties by imposing administrative sanctions in the form of:

- written warnings;
- temporary restriction / suspension of its business activities;
- administrative fines (in coordination with the relevant sector’s regulatory authority). The regulation does not specify the amount of administrative fines or the procedure to impose such fines;
- restriction to the access of the electronic system and/or information / data; and / or
- the business actor being excluded from certain registration list, and / or
- online publication in the website.

The ultimate sanction in MOCI Reg. 5/2020 is the blocking of access to the private electronic system operator’s (PSE’s) electronic systems in Indonesia. Access can be granted again once the private PSE has fulfilled its obligations.

However, as mentioned earlier, it does not rule out the possible enforcement by:

- other relevant sector’s regulatory authority (in the event the data controller / processor is subject to a regulated sector) which may also impose certain other administrative sanctions; and / or
- the law enforcement agency (prosecutor) if the non-compliance implies a criminal offense, which may subject the accused with imprisonment and / or fines.

Banking Law

Under Article 47 paragraph (2) of the Banking Law, any commissioner, director or employee of a bank or its affiliates who intentionally provides information which has to be kept confidential may be sentenced to imprisonment for not less than two (2) years but not more than four (4) years, and fined at least IDR 4 billion (±USD267,000) but not more than IDR 8 billion (±USD534, 000).

Capital Market Law

Under the Capital Market Law, the FSA is empowered to impose the following administrative sanctions for breaches of the provisions dealing with data protection. The sanctions include:

- A written reminder;
- A fine;
- Limitations on business;
- Suspension of business;
- Revocation of business license;
- Cancellation of approval; and / or
- Cancellation of registration.

Right to file a complaint

The PDP Law provides personal data subjects with the right to file a complaint against automated decision making.

Under the General Data Protection Regulations, an affected individual has the right to file a civil claim to the relevant electronic system operator (data controller / data processor) for losses incurred. On the other hand, it is also provided with the right to make complaints related to data protection infringements to the Directorate General for Informatics Application (*Direktorat Jenderal Aplikasi Informatika* or commonly abbreviated as "**DITJEN APTIKA**") within the MOCI in the event that there has been:

- no written notification made by the electronic system operator (data controller / processor) to the data subject concerning a data breach; or
- losses have been incurred by the data subject due to a data breach.

In addition, the general right to file a complaint is embedded in the Indonesian Civil Code, which provides that any party may claim for civil liability if any loss suffered may be evidenced to be resulting due to another party’s unlawful act.

ELECTRONIC MARKETING

The PDP Law and the General Data Protection Regulations do not specifically address electronic marketing.

Similar with other processing activities of personal data, a legal basis shall be available for conducting (electronic) marketing activities, (e.g. consent of the personal data subject).

It is interesting to note that one of the reasons for the introduction of the right to withdraw consent under the PDP Law was to enable personal data subjects to avoid (further) personal data breach occurrences which have emerged due to, among others, direct marketing practices.

ONLINE PRIVACY

There are currently no laws and regulations concerning cookies and location data.

Insofar the data generated through cookies or other tracking technologies, do not contain personal data, the use of thereof is generally permitted. Conversely, if any such cookies or tracking technologies do collect / generate personal data, then the use thereof shall be subject to the prevailing laws and regulations on personal data protection.

KEY CONTACTS

Tumbuan & Partners

Jennifer B. Tumbuan
Senior Partner
Tumbuan & Partners

jennifer.tumbuan@tumbuanpartners.com

Lingkan S. Ngantung
Partner
Tumbuan & Partners
lingkan.ngantung@tumbuanpartners.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

IRAN

Last modified 23 May 2019

LAW

Iran has not enacted comprehensive data protection legislation. However, several laws and regulations incorporate data protection provisions.

These include:

- Sharia law principles
- The Constitution of the Islamic Republic of Iran
- Draft of the Bill on Protection of Data and Privacy in the Cyber Space 2018
- Charter of Citizen’s Rights 2016
- Cyber Crime Act 2011
- The Law Concerning Protection of Consumers Rights 2010
- The Law on Publishing and Access to Data 2010
- Stock Market Law 2006
- Electronic Commerce Law (ECL 2004)
- The Law on Facilitation of Competition and Prevention of Monopoly 2004
- The Law on respect for Legitimate Rights and Citizen Rights 2004
- The Law on Establishment of the Ministry of Justice Official Experts 2003
- Press Law 2001
- Criminal Code 1997
- Bylaw Concerning Official Translators 1996
- Criminal Procedures Code 1994
- Direct Taxation Act as amended 1988
- The Law on Statistic Centre of Iran1976
- Civil Liability Code 1960
- The Law on Establishment of Notary Public Offices 1937
- Iranian Bar Association Law 1936

DEFINITIONS

Definition of Personal Data

Not specifically defined.

Under the Law on Publishing and Access to Data, “personal data” means first and last name, home and work address, individual habits, bank accounts information, etc.

The E-Commerce Law defines “private data” as a “data message” associated with a specific data subject. “Data message” means any representation of facts, information, and concepts generated, sent, received, stored or processed by use of electronic, optical or other information technology means.

Definition of Sensitive Personal Data

Not specifically defined.

Under the E-Commerce Law “sensitive personal data” has customarily been understood to mean data relating to family matters, criminal records, tribal or ethnic origins, moral and religious beliefs, ethical characteristics, sexual habits and data regarding health, physical or psychological status.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in Iran.

REGISTRATION

There is no registration requirement.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

Data collection and processing, including publication, is subject to data subject consent, provided that the “data message” is otherwise in accordance with Iranian law.

The collection and processing of personal "data messages" via electronic means is subject to the following conditions:

- the purpose of collection and processing must be specified and clearly described
- data may only be collected to the extent necessary to achieve its purported purpose
- “data messages” must be correct and up-to-date
- data subjects must be provided with access to computer files that contain “data messages” that concern the data subject
- data subjects must be provided with the ability to delete or rectify “data messages,” in accordance with relevant regulations (Article 59, E-Commerce Law)

Unless otherwise provided by law, the following is prohibited: searching, collecting, processing, using or disclosing personal data. This prohibition also applies to other mail and telecommunications, including telephone communications, faxes, wireless and private internet communications.

TRANSFER

The Charter of Citizen’s Rights prohibits personal data transfers without express data subject consent.

Under the ECL, third party and extraterritorial data transfers are subject to:

- data subject consent
- assurance that adequate security levels are in place to protect personal data in accordance with data subject rights and freedoms

SECURITY

Generally, Iranian business are required to take reasonable measures to secure personal information. It is unclear whether such measures must be physical, technical or organizational.

Nevertheless, somehow effective regulations apply to some businesses which are involved in sensitive information such as judges, attorneys, doctors, hospitals and pharmacies.

Under the ECL, “secure information system” is defined as an information system that:

- is reasonably protected against misuse or penetration
- possesses a reasonable level of proper accessibility and administration
- is reasonably designed and organized in accordance with the significance of the task
- is in compliance with secure methods

A “secure method” is a method to authenticate “data message” date, correctness, origin and destination, as well as to detect errors and modifications in its communication, content, or storage from a certain point. A secure message is generated using algorithms or codes, identification words or numbers, encryption, acknowledgement call-back procedures or similar secure techniques.

BREACH NOTIFICATION

There is no requirement to report data breaches to any individual or regulatory body.

ENFORCEMENT

Iranian courts generally enforce violations through statutorily defined remedies of the applicable law or regulation.

For example, the Cyber Crime Act provides that anyone who, by use of computer or telecommunication means, publicizes or makes accessible another individuals film, pictures or sounds, or personal or family secrets without consent, and causes loss or damage to the individual or violates that person’s dignity will be sentenced to imprisonment between 61 days and six months or fined RIs 1,000,000 to 10,000,000.

ELECTRONIC MARKETING

There is no specific electronic marketing law in Iran. However, under the Charter of Citizen’s Rights, operators must obtain addressee consent before sending any advertisement. Personal cell phones are considered as a private zone. Sending any unwanted advertisements, or spam, is against the law.

ONLINE PRIVACY

There is no specific online privacy law in Iran.

KEY CONTACTS

Dr. Hassan Sedigh
CEO
Sedigh & Associates Petroleum Consultants
T +98 21 22009042 - 3
sedigh@sa-petroleum.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

IRELAND

Last modified 11 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Irish Data Protection Act 2018 (“**DP Act**”) came into force on 25 May 2018 in order to give further effect to the GDPR in Ireland. The DP Act includes certain derogations, provides for the establishment of a new Data Protection Commission, implements the Law Enforcement Directive and otherwise addresses procedural aspects of the enforcement of data protection in Ireland.

The previous data protection legislation in Ireland, the Data Protection Acts 1988 to 2003, were largely repealed by the DP Act, however those Acts continue to apply in relation to certain limited purposes including national security and defence. Additionally, the previous legislation continues to apply in relation to complaints or infringements which occurred prior to 25 May 2018 as well as to investigations commenced (but not completed) prior to that date.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

"Public authority" and "public body" are terms used in the GDPR. For the purposes of the DP Act, the definition of a “**public body**” includes a company (and its subsidiaries) in which the majority of shares are held by or on behalf of a Minister of the Government.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The DP Act established the Data Protection Commission (“**DPC**") to act as the supervisory authority for data protection law in Ireland.

As well as supervising many domestic Irish businesses and organisations, the DPC also regulates many international and multi-national companies under the GDPR’s main establishment (or “one-stop shop”) regulatory mechanism.

Ireland has had one acting Commissioner for Data Protection, Helen Dixon, who served two five-year terms. However, the DP Act provides that the DPC can consist of up to three members. The Government, during July 2022 approved the commencement of the process to appoint two additional Commissioners. It is expected that at least two Commissioners will be appointed from 2024 onwards. In the event that there is more than one Commissioner, one of the Commissioners will be appointed as Chairperson.

The contact details of the DPC (or *An Coimisiún um Chosaint Sonraí*) are as follows:

Dublin office

21 Fitzwilliam Square South
Dublin 2, D02 RD28
Ireland

Regional office

Canal House
Station Road
Portarlington
R32 AP23 Co. Laois
Ireland

Website

www.dataprotection.ie

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

There is no general requirement in Ireland for controllers or processors to register their processing activities with the DPC, however, a register of Data Protection Officers (DPOs) is maintained.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

Ireland has not yet extended the requirement to appoint a Data Protection Officer (“**DPO**”). However, Section 34 of the DP Act does provide the Minister for Justice and Equality with the power to make regulations requiring controllers or processors to designate a data protection officer.

In addition, the DP Act requires enhanced “suitable and specific” measures to be implemented in relation to certain processing activities. In such cases, the designation of a DPO (in cases where it is not mandatory under GDPR) is listed in section 36 of the DP Act as one example of such measures.

The DPC maintains a register of DPOs. No fee is charged for registering or updating the details of a DPO.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");

- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known as lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

1. necessary for entering into or performing a contract;
2. authorized by EU or Member State law; or

3. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Part 3 of the DP Act sets out a range of national derogations as provided for in GDPR. Some of the notable provision include the following.

Processing for purpose other than purpose for which data collected

Section 41 of the DP Act permits the processing of personal data or special categories of personal data for purposes other than for which it was collected where necessary and proportionate for the purposes of: (a) preventing threats to national security, defence or public security; (b) preventing detecting, investigating or prosecuting crime; (c) providing / obtaining legal advice; (d) in connection with legal claims or prospective claims; or (e) establishing, exercising or defending legal rights.

Special category data

Chapter 2 of Part 3 governs the processing of special category personal data. The DP Act permits the processing of special category in certain circumstances including:

- for employment / social welfare law purposes;
- in relation to legal advice and proceedings;
- in the course of electoral activities;
- for the purposes of the administration of justice;
- for certain insurance or pension purposes as well as in relation to the mortgaging of a property;
- for reasons of substantial public interest;
- by health care workers for medical, health and social care purposes;
- in the interests of public health; and
- for archiving, scientific, historic or statistical purposes.

In most such cases, the DP Act requires enhanced “suitable and specific” measures to be implemented in order to protect the rights and freedoms of data subjects. The DPC has the right to request evidence of such measures, which can include:

- explicit consent of the data subject;
- limitations on access to the personal data;
- strict time limits for erasure of the personal data;
- specific training for those processing the personal data;
- various enhanced technical and organisational measures such as encryption and pseudonymisation; and
- processes and procedures for risk assessment purposes.

Health research regulations

The Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018 came into force in August 2018. The Health Research Regulations introduced material changes to the rules governing how health research can be conducted in Ireland and include:

- a new statutory definition of “health research”;
- a prescribed list of mandatory “suitable and specific measures” that must be adopted when processing personal data for health research purposes, including a general requirement that “explicit consent” be obtained from data subjects; and
- a list of exceptional circumstances in which the explicit consent requirement is not required and a detailed process to be followed in such cases.

Article 10 (criminal records) data

The DP Act expands the definition of Article 10 data to include personal data relating to the alleged commission of an offence and any proceedings relating to such offence. Section 55 of the DP Act provides for Article 10 (i.e. criminal records) data to be lawfully processed in a number of limited circumstances including:

- where the data subject has given explicit consent;
- where necessary and proportionate for the performance of a contract to which the data subject is party;
- where necessary for providing / obtaining legal advice or in connection with legal claims or prospective claims;
- where necessary for establishing, exercising or defending legal rights; or
- where necessary to prevent injury or damage or otherwise to protect vital interests.

The DP Act also requires enhanced “suitable and specific” measures to be taken to safeguard the rights and freedoms of data subjects in all of the above circumstances.

Children & child's consent to information society services

The DP Act defines a "child" as a person under 18 (this is relevant for example in assessing whether or not a data protection impact assessment may be required).

The DP Act provides that the digital age of consent in Ireland is 16 years old. This means that in order for any personal data pertaining to a child below the age of 16 to be processed in relation to an information society service, the consent of a parent or guardian is also required. The DPC ran two public consultations in 2019 on the processing of children’s personal data and the rights of children as data subjects and published the “Fundamentals for a Child-Oriented Approach to Data Processing” in December 2021. The DPC also has a statutory function, under section 32 of the DP Act, to encourage the drawing up of codes of conduct for the protection of children.

Section 33 of the DP Act provides a specific right of erasure for children in connection with personal data collected in relation to the offer of information society services.

The DP Act includes a prohibition on the processing of children's personal data for the purposes of direct marketing, profiling and micro-targeting. Section 30 has however not been commenced due to concerns that enacting it would place Ireland in breach of EU law.

Automated decision making

Section 57 of the DP Act provides for a derogation whereby the right under GDPR not to be subject to a decision based solely on automated decision-making including profiling where the decision is authorised or required under an enactment and either (1) the effect of the decision is to grant a request of the data subject, or (2) adequate steps have been taken to safeguard the legitimate interests of the data subject.

Rights of data subjects

Section 60 of the DP Act sets out the circumstances in which data subject rights may be restricted. These include where such restrictions are necessary and proportionate:

- to safeguard cabinet confidentiality, parliamentary privilege, national security, defence and the international relations of the State;
- for the prevention, detection, investigation and prosecution of criminal offences;
- for the administration of taxes or duties;
- for the establishment, exercise or defence of, a legal claim or prospective legal claim;
- for the enforcement of civil law claims; or
- for the purposes of estimating the amount of the liability of a controller on foot of a claim.

Section 60 also restricts data subject rights to the extent that the personal data relating to the data subject is an expression or opinion by another person given in confidence, or on the understanding that it would be treated as confidential. The person in receipt of the information must have a legitimate interest in receiving the information.

Data subject rights can also be restricted in relation to information which is subject to legal privilege.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, South Korea, United Kingdom, Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on the condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others: binding corporate rules, standard contractual clauses and the EU-US Privacy Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

1. explicit informed consent has been obtained;
2. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
3. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
4. the transfer is necessary for important reasons of public interest;
5. the transfer is necessary for the establishment, exercise or defence of legal claims;
6. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
7. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

Section 37 of the DP Act provides the Minister for Justice and Equality with the power to make regulations restricting the transfer of categories of personal data to a third country or an international organisation for important reasons of public policy.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

1. the pseudonymization and encryption of personal data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The DP Act requires enhanced “suitable and specific” measures to be implemented in relation to certain processing activities. In such cases, enhanced data security measures (including logs / audit trails and encryption) are listed in section 36 of the DP Act as one example of such measures.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

Personal data breaches should be notified to the DPC which has a published web form and risk rating requirement for personal data breach notifications.

The online breach reporting web form requires specific information to be provided depending on whether the personal data breach is a national or cross-border breach (in the latter case where the DPC acts as the lead supervisory authority

under GDPR’s main establishment (or “one-stop shop”) regulatory mechanism). Further specific information is required to be provided for telecommunications and internet service providers to report breaches under Commission Regulation (EU) No 611/2013.

Organisations reporting breaches are requested to provide a self-declared risk rating using the following thresholds:

- *Low Risk*: The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal.
- *Medium Risk*: The breach may have an impact on individuals, but the impact is unlikely to be substantial.
- *High Risk*: The breach may have a considerable impact on affected individuals.
- *Severe Risk*: The breach may have a critical, extensive or dangerous impact on affected individuals.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Enforcement powers

Part 6 of the DP Act provides the DPC with a wide-range of powers to supervise organisations under its jurisdiction, including:

- Powers to handle complaints made (directly or indirectly) to it;
- Powers to open and conduct “own-volition” inquiries;
- Powers to issue decisions and exercise corrective powers (including administrative fines) provided for in GDPR;
- Powers to issue a variety of corrective orders including warnings, reprimands, directions, suspensions or restrictions;
- Powers of entry, search, seizure and inspection, including the removal and retention of documents or records;
- Powers to issue information and enforcement notices; and
- Powers to require an organisation to carry out a report or audit.

Criminal offences

The DP Act provides for several offences which can result in prosecution, imprisonment, and criminal penalties being imposed. Where offences are committed by an organisation, and such offence is committed with the consent, connivance or negligence of a manager, director, secretary or other officer of the company, the individual will be personally liable for the offence, as well as the organisation. The offences under the DP Act include:

- an employer or potential employer forcing an individual to make a subject access request;
- a processor disclosing personal data without the consent of the controller unless required to do so by law;
- obtaining and disclosing, or selling personal data to a third party without the consent of the relevant controller or processor of that data, or in relation to data which were unlawfully disclosed to them;
- contravening the provisions relating to the processing of criminal convictions and offences data;
- not cooperating with an authorised officer during an investigation, audit or inspection; and
- failing to comply with an information or enforcement notice.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The ePrivacy Regulations implement the anti-spam rules set out in Article 13 of the Privacy and Electronic Communications Directive 2002/58/EC (as amended by the Citizens’ Rights Directive). These regulations came into effect on 1 July 2011. Electronic mail includes text messages (SMS), voice messages, sound messages, image messages, multimedia message (MMS) and email messages.

Direct marketing emails can generally only be sent to users with their prior consent. A limited exemption is available for direct marketing emails sent to existing customers promoting other products or services similar to those previously purchased by that consumer (such emails can only be sent for 12 months, the customer must have been given the opportunity to object when the details were collected and the product or service being marketed must be a product or service offered by the person with the existing relationship with the customer). B2B direct marketing emails can generally be sent unless the recipient has informed the sender that it does not consent to the receipt of such messages.

The identity of the sender must not be disguised or concealed and the recipient must be offered an opt-out.

Direct marketing calls (excluding automated calls) may be made to a landline provided the subscriber has not previously objected to receiving such calls or noted his or her preference not to receive direct marketing calls in the National Directory Database.

Direct marketing calls cannot be made to a mobile phone without prior consent.

One cannot send a direct marketing fax to an individual subscriber in the absence of prior consent. One can send such a fax to a corporate subscriber unless that subscriber has previously instructed the sender that it does not wish to receive such communications or has recorded a general opt-out to receiving such direct marketing faxes in the National Directory Database.

Breach of these anti-spam rules is a criminal offence. On a summary prosecution (before a judge sitting alone) a maximum fine of EUR 5,000 per message sent can be handed down. On conviction on indictment (before a judge and jury) a company may be fined up to EUR 250,000 per message sent and an individual may be fined up to EUR 50,000 per message.

The GDPR applies to most electronic marketing activities, as these will typically involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47 of GDPR). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and

marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (“**ePrivacy Directive**”), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation though there remains uncertainty at an EU level as to when this legislation will be passed. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46 /EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

In Ireland, the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (“**ePrivacy Regulations**”) implement the rules on electronic direct marketing set out in the ePrivacy Directive.

Direct marketing emails (which includes SMS and other text, voice, sound or image messages) can generally only be sent to users with their prior (opt-in) consent.

Two exemptions are available whereby emails can be sent on an opt-out basis:

Customer exception

Direct marketing emails may be sent on an opt-out basis to an existing customer promoting similar products or services to those purchased by that customer. Such emails can only be sent for 12 months from the date of sale to the customer, the customer must be given the opportunity to object both (1) when the details were collected, and (2) in each marketing message. Moreover, the product or service being marketed must be a product or service offered by the person with the existing relationship with the customer.

B2B exception

Business to business (**"B2B"**) direct marketing emails can generally be sent unless the recipient has informed the sender that it does not consent to the receipt of such messages. To qualify for the B2B exception, an email address must reasonably appear to the sender to be an email address used mainly by the recipient in the context of their commercial or official activity and the marketing message must relate solely to that commercial or official activity.

ONLINE PRIVACY

Cookies

Consent is needed for the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user. A user must be provided with ‘clear and comprehensive information’ about the cookie (including, in particular, its purposes). This information must be prominently displayed and easily accessible. The methods adopted for giving information and obtaining consent should be as ‘user friendly’ as possible. The DPC has provided regulatory guidance on cookies and other tracking technologies which can be accessed here.

Location Data

One cannot process location data unless either:

- such data has been made anonymous; or
- user consent has been obtained.

A provider of electronic communication networks or services or associated facilities (i.e. a telco) must inform its users of:

- the type of location data (other than traffic data) that will be processed;
- the purpose and duration of the processing; and
- whether the data will be transmitted to a third party to provide a value added service. Users can withdraw their consent to the processing of location data.

Cookies

The use of cookies (and similar technologies) is regulated by the GDPR as well as the ePrivacy Regulations.

The ePrivacy Regulations provide that a person shall not use an electronic communications network to store information, or to gain access to information already stored in the terminal equipment of a subscriber or user, unless (1) the subscriber or user has given his or her consent to that use, and (2) the subscriber or user has been provided with clear and comprehensive information which (a) is both prominently displayed and easily accessible, and (b) includes, without limitation, the purposes of the processing of the information.

The DPC’s guidance has confirmed that all cookies and tracking technology tools require consent, apart from two exceptions:

- **Communications exemption** – a cookie whose sole purpose is to carry out the transmission of a communication over a network; and
- **Strictly necessary exemption** – this applies to a service delivered over the internet (e.g. websites or apps) which have been explicitly requested by the user and the use of cookies is restricted to what is strictly necessary to provide that service.

The DPC commenced enforcement action on compliance with its regulatory guidance for controllers in October 2020.

Location data

The ePrivacy Regulations deal with the collection and use of location and traffic data by electronic communications network and service providers. Location data other than traffic data relating to users or subscribers of undertakings can only be processed if (1) such data are made anonymous, or (2) the consent of the users or subscribers has been obtained to the extent and for the duration necessary for the provision of a value added service.

KEY CONTACTS

John Magee
Partner
T +353 1 436 5450
john.magee@dlapiper.com

Eilis McDonald
Senior Associate
T +353 1 436 5479
eilis.mcdonald@dlapiper.com

Sarah Dunne
Associate
T +353 14 876699
sarah.dunne@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ISRAEL

Last modified 22 December 2023

LAW

The laws that govern the right to privacy in Israel are the Basic Law: Human Dignity and Liberty, 5752 -1992; the Protection of Privacy Law, 5741-1981 and the regulations promulgated thereunder (the 'PPL') and the guidelines of the Israel Privacy Authority (as defined below).

DEFINITIONS

Definition of personal data

Personal Data, as defined under the PPL, means: data regarding the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person.

Definition of sensitive personal data

Sensitive Data, as defined under the PPL, means: data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person; and other information if designated as such by the Minister of Justice with the approval of the Constitution, Law and Justice Committee of the Knesset. No such determination has been made to date.[1]

1: On July 23, 2020, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Definitions and Limiting Registration Obligations) 5782- 2021. The draft bill proposes to revise defined terms under the PPL to align with the definition in the GDPR, such as definition of: personal data, sensitive data, processing, owner of a database, holder of a database and other. In addition, the draft bill attempts to limit database registration requirements to apply to certain categories of databases containing information of 100,000 data subject or more. The draft bill has yet to be placed on the table of the Israel Knesset for its first reading. Furthermore, the draft bill expands the administrative enforcement of the IPA. On May 18, 2021, the Israeli Ministry of Justice published two draft bills proposing to amend the PPL (Appointment of an Official Representative) 5782-2021 and the PPL (Minor's Privacy) 5782-2021. On July 26, 2021, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Limitation Period) 5721-2021 to extend the limitation period by which a civil claim may be filed under the PPL from a period of two years to a period of seven years, in accordance with the Statute of Limitations Law 5718-1958. All the foregoing draft bills have been placed on the table of the Israel Knesset and for their preliminary discussion. On January 5, 2022, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Amendment Number 14) 5782-2021. The draft bill proposes to increase the supervisory and enforcement capabilities of the IPA (such as impose financial sanctions for violating the provisions of the law concerning the management of databases up to an amount of NIS 3.2 million), to reduce the obligation to register databases as well as to adapt the defined terms under the Israel Protection of Privacy Law to the technological developments and modern privacy legislation. The draft bill has been approved in its first reading of the Israel Knesset and is in preparation for the second and third reading in the Knesset committee. On January 31, 2022, the Israeli Ministry of Justice published a draft bill proposing to

amend the PPL (Strengthening the Right to Privacy and its Protection) 5782-2021. The draft bill proposes additional rights of data subjects to control their personal information. In addition, the draft bill includes further strengthening of the enforcement powers of the IPA, in particular with regards to enforcement on an international level. The draft has been set on the Knesset's table for its first reading. On January 31, 2022, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Deletion from Databases), 5782-2022. The draft bill proposes to add requirements to the notification obligations to data subjects, prior to collecting personal information (Section 11 of PPL), such as adding an obligation to indicate when a renewed authorization to hold the personal information will be requested and deleting the personal information either by the data subject contacting the owner of the database, or automatically if five years have passed since receiving a notification, and no renewed authorization to hold the personal information was received. The draft bill has been approved in its first reading of the Israel Knesset and is awaiting the Knesset committee to appoint a handling committee.

On February 16, 2023, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL: (Prohibition on Publishing a Recording of an Individual) 5783- 2023, which proposes to prohibit publishing a recording of an individual in public which contains Sensitive Data. The draft bill has been placed on the table of the Israel Knesset and for its preliminary discussion.

NATIONAL DATA PROTECTION AUTHORITY

The Israel Privacy Authority ("**IPA**"), established in September 2006, as determined by Israel's Government decision no. 4660, dated 19.01.2006.

REGISTRATION

Subject to certain exceptions, database registration is required to the extent one of the following conditions are met[1]:

- the database contains information in respect of more than 10,000 data subjects;
- the database contains sensitive information;
- the database includes information on persons, and the information was not provided by them, on their behalf or with their consent;
- the database belongs to a public entity; or
- the database is used for direct marketing services.

A database is defined under the PPL as a collection of data, stored by magnetic or optic means and intended for computer processing, consequently excluding noncomputerized collections.

In 2005, the Ministry of Justice set up a committee generally known as the 'Schoffman Committee' which recommended relaxing registration of 'ordinary' databases and focusing on specific categories of information (e.g. medical data, criminal records or information about a person's political or religious beliefs). However, to date, the Schoffman Committee recommendations have not crystallized into binding legislation.

On November 11, 2018, the IPA published *Opinion: Is the Collection of Names and Emails Considered a “Database”?* in which the IPA ruled that a list of emails is deemed Personal Data.

1: On July 23, 2020, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Definitions and Limiting Registration Obligations) 5782- 2021. The draft bill proposes to revise defined terms under the PPL to align with the definition in the GDPR, such as definition of: personal data, sensitive data, processing, owner of a database, holder of a database and other. In addition, the draft bill attempts to limit database registration requirements to apply to certain categories of databases containing information of 100,000 data subject or more. The draft bill has yet to be placed on the table of the Israel Knesset for its first reading. Furthermore, the draft bill expands the administrative enforcement of the IPA. On May 18, 2021, the Israeli Ministry of Justice published two draft bills proposing to amend the PPL (Appointment of an Official Representative) 5782-2021 and the PPL (Minor's Privacy) 5782-2021. On July 26, 2021, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Limitation Period) 5721-2021 to extend the limitation period by which a civil claim may be filed under the PPL from a period of two years to a period of seven years, in accordance with the Statute of Limitations Law 5718-1958. All the foregoing draft bills

have been placed on the table of the Israel Knesset and for their preliminary discussion. On January 5, 2022, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Amendment Number 14) 5782-2021. The draft bill proposes to increase the supervisory and enforcement capabilities of the IPA (such as impose financial sanctions for violating the provisions of the law concerning the management of databases up to an amount of NIS 3.2 million), to reduce the obligation to register databases as well as to adapt the defined terms under the Israel Protection of Privacy Law to the technological developments and modern privacy legislation. The draft bill has been approved in its first reading of the Israel Knesset and is in preparation for the second and third reading in the Knesset committee. On January 31, 2022, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Strengthening the Right to Privacy and its Protection) 5782-2021. The draft bill proposes additional rights of data subjects to control their personal information. In addition, the draft bill includes further strengthening of the enforcement powers of the IPA, in particular with regards to enforcement on an international level. The draft has been set on the Knesset's table for its first reading. On January 31, 2022, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Deletion from Databases), 5782-2022. The draft bill proposes to add requirements to the notification obligations to data subjects, prior to collecting personal information (Section 11 of PPL), such as adding an obligation to indicate when a renewed authorization to hold the personal information will be requested and deleting the personal information either by the data subject contacting the owner of the database, or automatically if five years have passed since receiving a notification, and no renewed authorization to hold the personal information was received. The draft bill has been approved in its first reading of the Israel Knesset and is awaiting the Knesset committee to appoint a handling committee.

On February 16, 2023, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL: (Prohibition on Publishing a Recording of an Individual) 5783- 2023, which proposes to prohibit publishing a recording of an individual in public which contains Sensitive Data. The draft bill has been placed on the table of the Israel Knesset and for its preliminary discussion.

DATA PROTECTION OFFICERS

Appointment of a Data Protection Officer is required by an entity meeting one of the following conditions:

- a possessor of five databases that require registration;
- a public body as defined in Section 23 to the PPL; or
- a bank, an insurance company or a company engaging in rating or evaluating credit.

Failure to nominate a Data Protection Officer when required to do so may result in criminal sanctions, including administrative fines. The PPL does not require that the Data Protection Officer should be an Israeli citizen or resident.

In the event that a data protection officer was appointed pursuant to the PPL, the Israel Protection of Privacy Regulations (Data Security), 5777-2017 ('Data Security Regs') require that the officer be directly subordinate to the database manager, or to the manager of the entity that owns or holds the database. In addition, the Data Security Regs prohibit the officer from being in a conflict of interest and require the officer to establish data security protocols and ongoing plans to review compliance with the Data Security Regs. The officer must present findings from such review to the database manager and its supervisor.

COLLECTION & PROCESSING

The collection, processing or use of Personal Data is permitted subject to obtaining the informed consent of the data subjects. Such consent should adhere to purpose, proportionality and transparency limitations. As such, consent should be obtained for specific purposes of use, the processing and use of Personal Data should be proportionate to those purposes, and data subjects should have the right to inspect and correct their personal information. The data subject's consent must be reobtained for any change in the purpose of use.

Any request for consent from a data subject to have his or her Personal Data stored and used within a database must be accompanied by a notice indicating:

- whether there is a legal requirement to provide the information;
- the purpose for which the information is requested;
- the recipients of the data; and
- the purpose(s) of use of the data.

Retaining outsourcing services for the processing of personally identifiable information is subject to the IPA's Guidelines on the Use of Outsourcing Services of Processing Personal Information (Guideline 2/2011) dated 10 June 2012 ('Outsourcing Guidelines'). The Outsourcing Guidelines include, inter olio, factors to be taken into consideration when deciding to use outsourcing services, specific provisions to be included within the data transfer agreement and data security requirements. Processing of personally identifiable information in certain sectors is subject to additional outsourcing requirements.

Furthermore, the Outsourcing Guidelines also require compliance with the Data Security Regs.

Entities subject to separate outsourcing guidelines are for example entities supervised by the Commissioner of the Capital Market, Insurance and Savings and entities supervised by the Banking Supervision Department of the Bank of Israel. On 10 September 2014, the Banking Supervision Department of the Bank of Israel issued draft guidelines regarding risk management in cloud computing services used by Israeli banking corporations. Among other various restrictions, the draft guidelines set forth an obligation on supervised entities to receive the approval of the Supervisor of Banks prior to using cloud computing services. The general issue of privacy consideration in the use of surveillance cameras is governed by the IPA Use of Surveillance Cameras and the Footage Obtained Therein Guidelines (no. 4/2012). In 2017, the IPA published Use of Surveillance Cameras in the Workplace and in Working Relationships Guidelines (no. 5/17) specifically referring to the use of surveillance cameras in the workplace. The guidelines state that the employer's prerogative to use surveillance means in the workplace is subject to fulfillment of principals such as legitimacy, transparency, proportionality, good faith and fairness. These principles apply also to businesses required by law enforcement to place surveillance cameras on their premises. The guidelines specify the manner in which these principles should be implemented, derivative requirements and possible implications.

On December 27, 2018. The Camera Installation Law for the Protection of Toddlers in Day Care Centers for Toddlers (5779 - 2018) was published and became effective on September 1, 2020. The said law provides that the operator of a daycare center for toddlers is required (unless it falls under the exceptions under the law) to install cameras that will record during the time of which the toddlers are present, without sound. It is forbidden to view the videos, to copy them, to transfer them to another person and to make any use of them without a court order (except for the Police and the Ministry of Welfare officials for the purpose of preventing harm to toddlers that are in the daycare). No real-time viewing of the footage is permitted, and it must be deleted withing 30 days from the date of filming.

On July 8, 2023, the Israeli Ministry of Justice published: Amendment to Installation of Cameras for the Protection of Toddlers in Daycare Centers for Toddlers (Amendment No. 1), 5779 -2017, which intends to strike a balance between the need to protect toddlers and the need to reduce as much as possible the harm to the privacy of the toddlers and the daycare staff, usually from photographing and viewing the photographs. The draft bill has been placed on the table of the Israel Knesset and for their preliminary discussion.

On October 16, 2023, The IPA published Publication: Protecting the Privacy of Students in Distance Learning, which presents a number of emphases and recommendations for proper conduct and protection of privacy and Personal Information as part of students' use of online distance learning applications.

Furthermore, on March 29, 2020 its Recommendations: Privacy Aspects of Use of Drones which, recommends that the drone user take into account alternatives that will not violate the privacy of others and to activate the drone proportionately in order to minimize the scope of Personal Data collected, processed and stored. The period in which the Personal Data is retained should be limited as much as possible and for as long as the Personal Data is stored on the drone, the drone is to be kept in a physically safe location; ensure privacy by design and compliance with the PPA requirements in respect of privacy by notification, transparency and deletion of data.

On August 31, 2021, the IPA published Draft Guidelines: Collection of Employee Location Data Using Dedicated Apps and Vehicle Location Systems. The guidelines emphasize that such a use shall only be made in the absence of an alternative. The employer must further determine in advance the purpose, the specific range of hours Personal Data collection, and the duration for which the information will be retained.

On May 22, 2023, the IPA published Publication: Privacy Related Aspects of Monitoring Remote Working Employees, which includes certain standards required for employers that monitor their employees working remotely in order to avoid breach of their privacy rights (including without limitation compliance with proportionality and legitimacy standards such as limiting

surveillance solely to work hours; employers must inform their employees that they are using technological means to monitor their behavior when working remotely, including the purpose for which the monitoring is done).

On July 26, 2023, the IPA published Opinion: Collecting Location Data of Employees Using Applications and In-Vehicle Tracking Systems, which determines guidelines on how to collect such data from employees in their vehicles provided by the employer.

On March 25, 2021, the IPA published Policies of Data Minimization, which require database owners to: ensure that the information collected is and will be required to achieve the purpose of for which it was collected and is deleted thereafter; check annually if they possess data that is irrelevant etc.

On December 12, 2022, the IPA published Guidelines: What are ‘Data’ and ‘Information on a Person’s Private Affairs’ according to the PPL, which clarifies the meaning of the terms Data and Information on a Person's Private Affairs.

On July 23, 2020, the Special Authorities to Combat the Novel Corona Virus (Temporary Order) 5780 – 2020 came into effect (by virtue of the Israel Government's authority under Section 39 of the Basic Law: The Government). Under the Temporary Order, and the authorities granted to the Israel General Security Service ('GSS') by the General Security Service Authorization Law 5762-2002, the Government may establish new regulations which potentially broaden Israel Government authorities / GSS rights in respect of collection and processing Personal Data, such as: the Emergency Regulations (General Security Service Authorization to Assist in the National Effort to Reduce the Spread of the Novel Corona Virus), 5780- 2020 which authorized the GSS to perform surveillance on Israel citizens to reduce the spread of the Corona Virus; Emergency Regulations (Location Data), 5780-2020 were established amending the Criminal Procedure Law (Enforcement Powers – Communication Data) 5768- 2007 authorizing the Israel Police to preform cell phone surveillance (i.e. receiving the location of a cell phone from a cellular operator) of a Corona virus patient without a court order; and the Emergency Regulation (General Security Service to assist in National Effort to Reduce Spread of Omicron Strain of Novel Corona Virus), 5782- 2021 that permit the GSS to perform surveillance of Israel citizens. The Temporary Order has been extended until February 15, 2024, in order to maintain a legal infrastructure that enables taking actions under the law to reduce the spread of the coronavirus and reduce harm to public health.

On January 2022, the IPA published Recommended Guidelines: Appointment of a Privacy Protection Officer ("PPO") and its Roles and Responsibilities. In Israel, there is no obligation to appoint a PPO, but the IPA recommends appointing one in organizations that collect and process Personal Data, databases owners and holders in a database. Appointing a PPO helps the organization verifying that it complies with the provisions of the PPL and the Data Security Regs and is indication that the organization has taken and takes steps to reduce the risk of damage to the Personal Data kept in its possession. In the recommended guidelines, the IPA refers to the scope of the PPO's role, which will be determined according to the complexity of the data processing operations carried out in the organization and according to its size. Also, the roles and tasks that are recommended to be under the care of a PPO are, among others, regulation of information management processes, supervision and control and training and implementation.

On July 31, 2022, the IPA published Obligation to Notify as Part of Collection and Use of Personal Information Guideline. The guideline requires notification to data subjects which their Personal Data is collected and used by systems for making algorithm-based or artificial intelligence decisions.

On February 20, 2023, the Committee of Ministers for Legislative Affairs published Amendment to the Police Order (No. 40) (Biometric Photographic System) 5783- 2023, which regulates aspects of placing systems that capture biometric photos in public spaces by the police. The photo systems include the capabilities to process the photos of people and compare them to identifiable information entered into the system, in a way that may allow indemnification.

On June 6, 2023, Inclusion of Biometric Identification Means and Biometric Identification Data in Identification Documents and in the Database (Amendment and Temporary Order), 5777-2017, came into effect, which allows the collection of fingerprints for the police's public biometric database, until June 30, 2024.

Furthermore, On October 14, 2023, the Israeli Ministry of Justice published Emergency Regulations: IDF Authorization to Perform an Operation on Computers Used for Activating Cameras, which authorize IDF soldiers (which have required skills) to penetrate and operate on computers used to operate stationary cameras, without receiving consent of the person who owns the computer, under certain circumstances, such as: the penetration of the computer: (i) is essential for preventing access to information, which has the potential to actually endanger the security of the state or the continuity of the operational functioning of the IDF; (ii) is required immediately and urgently; or (iii) it is not possible, in the timeframe to obtain the consent of the owner of the computer.

On November 15, 2023, The IPA published publication: Privacy in Home IoT Products and Smart Homes, which includes recommendations to companies that provide IoT (Internet of Things) services and products in the home space, as part of transforming homes into "smart homes" and to such users, as the smart home devices collects and processes a large amount of Personal Data and Sensitive Data and introduction of surveillance systems into the areas of the individual's private and intimate space.

On August 22, 2023, the IPA published Publication: Disclosure of Personal Information Regarding Male and Female Students on The Websites of Higher Education Institutions, which includes guidelines as to manner of such disclosure.

On December 11, 2023, the government published Memorandum of Law: Israel Security Agency (Amendment No....), 2023 open to comments by the public, which purpose is to regulate certain aspects including cyber and computers and to grant GSS rights to receive, collect and transmit information, including from databases, subject to certain approvals, supervision and control mechanisms. Which is in addition to the publication by the Israeli Ministry of Justice published on February 28, 2021 the draft bill Memorandum: "The Cyber Defense Law and the National Cyber System (Authorities for the Purpose of Strengthening Protection) (Temporary Order), 5781-2021", which states that the National Cyber System and the GSS will be permitted to give instructions to private and public organizations in Israel on how to prepare for and defend against a cyber-attack and addresses compliance issues.

On December 29, 2022, the IPA published Recommendations for Proper Conduct When Using Applications (Apps) to Pay and Validate Public Transportation, including without limitation recommendations in respect of privacy policies, app information security, deletion of Personal Data and other.

On January 24, 2023, the Israeli Ministry of Justice published Memorandum: "Health Information Mobility Law, 5783-2023", to regulate patient's access to their health information in connection with provision of health services while protecting their privacy and data security.

On August 8, 2023 the IPA published: The Right of Inspection Regarding the Databases of Entities Listed in Section 13(e) of The PPL, which grants individuals the right of inspection in respect of the databases of the entities listed in Section 13 (e) of the PPL (such as security authorities, prison service, tax authority, Minister of Justice, and other).

TRANSFER

The transfer of Personal Data abroad is subject to the Privacy Protection Regulations (Transfer of Data to Databases Abroad), 5761-2001 ("**Transfer Regs**"), pursuant to which Personal Data may be transferred abroad only to the extent that:

- the laws of the country to which the data is transferred ensure a level of protection, no lesser than the level of protection of data provided for by Israeli Law; or
- one of the following conditions is met:
  - the data subject has consented to the transfer;
  - the consent of the data subject cannot be obtained and the transfer is vital to the protection of his or her health or physical wellbeing;
  - the data is transferred to a corporation under the control of the owner of the database from which the data is transferred, provided that such corporation has guaranteed the protection of privacy after the transfer;

- the data is transferred to an entity bound by an agreement with the database owner, to comply with the conditions governing the use of the data as applicable under Israeli Laws, mutatis mutandis;
- data was made available to the public or was opened for public inspection by legal authority;
- transfer of data is vital to public safety or security;
- the transfer of data is required by Israeli Law; or
- data is transferred to a database in a country:
  - which is a party to the European Convention for the Protection of Individuals with Regard to Automatic Processing of Sensitive Data; or
  - which receives data from Member States of the European Community, under the same terms of acceptance[1], or
  - in relation to which the Registrar of Databases announced, in an announcement published in the Official Gazette (*Reshumot*), that it has an authority for the protection of privacy, after reaching an arrangement for cooperation with that authority.

When transferring personal data abroad, the database owner is required to enter into a data transfer agreement with the data recipient, pursuant to which the recipient undertakes to apply adequate measures to ensure the privacy of the data subjects and guarantees that the data shall not be further transferred to any third party.

The foregoing data transfer agreement must also comply with additional restrictions, to the extent that the recipient provides outsourcing services, as set forth in the Outsourcing Guidelines.

On January 31, 2011, the European Commission, on the basis of Article 25(6) of directive 95/46/EC, determined that the State of Israel ensures an adequate level of protection with regard to automated processing of personal data.

Additionally, the transfer of databases is subject to the IPA Draft Guidelines No. 3/2017, which under certain circumstances, such as database recipient having a conflict of interest, might require opt-in consents of data subjects as a condition to transferring databases.

On January 4, 2022, the IPA published a Draft Guideline: Interpretation of Section 3 of Transfer Regs, clarifying the prohibition on onward transfer of Personal Data by a data recipient stipulating that where the following applies, such onward transfer may be permitted: (i) written consent of the database owner; (ii) the transfer of the information to a third party is performed lawfully, that is, based on the consent of the data subjects or is required by law; and (iii) If the information was transferred directly from Israel to such third party, such transfer itself would comply with the conditions set forth above.

On November 29, 2022, the Ministry of Justice published for public comments draft regulations on data transferred from the EEA to Israel which include additional data subject rights such as: right to be forgotten and restrictions on data retention, as part of Israel's deference to maintain its adequacy level of protection received from the EU. Timing of the regulations entering into force is dependent on the new government being formed.

On May 7, 2023, the Israeli Ministry of Justice published Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 5783-2023, which establish obligations (such as: obligation to delete Personal Data, limit the retention of Personal Data that is not necessary, accuracy and notification obligations) that will apply to Personal Data transferred to Israel from the European Economic Area (EU, Iceland, Norway and Liechtenstein). Furthermore, information regarding a person's origin and information regarding membership in a labor organization will be considered Sensitive Data.

On September 14, 2023, the IPA published Manual: Contracting with Outsourcing Providers – Section 15 to the Data Security Regs, which clarifies the manner in which companies shall contract with their outsourcing providers. The manual specifies issues to be included in the binding agreement between the company and the outsourcing provider, and it includes two appendices for use by the parties: an auxiliary questionnaire for checking the information security aspects of the outsourcing provider, and a proposed questionnaire to determine the method of performing the periodic control of the outsourcing provider.

1: Following the decision of the ECJ in Case C362/14 Maximillian Schrems v Data Protection Commissioner, IPA issued a statement on October 15, 2015, according to which US safe harbour certified entities would not fall under the foregoing condition, without derogating from all other conditions. Similarly following the decision of the CJEH in the Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, IPA issued a statement on September 29, 2020, according to which US privacy shield certified entities would not fall under the foregoing condition, without derogating from all other conditions.

SECURITY

On March 21, 2017, the Constitution, Law, and Justice Committee of the Knesset approved the Data Security Regs, which have come into effect on May 2018. The Data Security Regs further broaden the PPL by imposing additional requirements applicable to database owners, holders and managers. Such additional requirements include, without limitation, having in place a broad list of manuals and policies; various physical, environmental and logical security measures; and regular audit, inspection and training obligations.

Furthermore, the Data Security Regs add to the Outsourcing Guidelines, which in effect would expand the requirements applicable when outsourcing processing services, even prior to entering into a data transfer agreement between the database owner and the data recipient and the requirements to be included therein.

Failure to comply with the Data Security Regs will constitute a breach of the PPL, which may expose a non-compliant entity to criminal and civil liability, as well as to administrative fines.

In March and April of 2018, the IPA published guidelines regarding the applicability of the Data Security Regs to four types of organizations: organizations certified to ISO/IEC 27001 standard, supervised entities subject to the directives of the Supervisor of the Bank, management companies and insurers which are subject to the provisions of the Capital Market, Insurance and Savings Authority and non-bank stock exchange members subject to stock exchange regulations. These types of organizations only need to comply with selective provisions of the Data Security Regs.

On May 1, 2018, the IPA published the Privacy Protection Authority’s Policy for Reporting Severe Security Incidents. The directive sets forth the instructions on how to report a severe security incident. Failure to comply with the directive may lead to sanctions such as advertising the violation or deletion of database registration.

On March 20, 2023, the IPA published Opinion: Security Risks in Shortened URLs, which describes the security risks arising from services that enable such shorten links to websites and recommends to avoid, unless a throughout security check has been conducted, not to apply such shortened links to a database of Personal Data and additional security related guidelines.

On September 7, 2023, the IPA published Guideline: The Role of The Board of Directors in Fulfilling The Corporation's Obligations According To The Privacy Protection Regulations (Information Security), which details the role of the board of directors in fulfilling the company's obligations according to the Data Security Regs. In companies which processing of Personal Data is at the core of their activity, or companies whose activity creates an increased risk of breaching privacy laws, the company's board of directors is the appropriate party to perform the duties set forth in the Data Security Regs.

BREACH NOTIFICATION

Pursuant to the Data Security Regs, data breach notifications are required depending on the severity of the breach and the category of the database. Such notifications are generally to the IPA which may require further notification to the data subjects.

On August 7, 2022 the IPA updated their data breach notification policy. The IPA requires immediate reporting not only upon discovery, but also when there is merely a concern about the existence of a Serious Information Security Incident (as defined in the PPL), as well as the steps to be taken following the incident.

ENFORCEMENT

IPA has the authority and obligation to supervise compliance and enforce the provisions of the PPL and appoint inspectors to carry out those activities.

Breach of the PPL may result in both civil and criminal sanctions, including administrative fines, 15 years of imprisonment, and the right to receive statutory damages under civil proceedings without the need to prove actual damages.

The current draft bill for the 13th Amendment of the PPL provides IPA with the ability to conduct criminal investigations and to impose monetary sanctions in the amount of up to NIS 3.2 million. The draft bill has passed its first reading, but has yet to pass the approval of the Knesset Constitution, Law and Justice Committee; thereafter it would need to also pass the second and third readings, in order to become a binding piece of legislation.

ELECTRONIC MARKETING

Unsolicited marketing is regulated under the Communications Law (Telecommunications and Broadcasting), 1982 (the 'Anti Spam Act'). The Anti Spam Act prohibits, subject to certain exceptions, advertising by means of automated dialing, fax or text messages without first obtaining the recipient's initial opt-in prior consent; all such communications also must contain an optout / unsubscribe option.

Furthermore, the PPL governs the possession and management of databases intended for direct mailing service and imposes restrictions in connection therewith, including a database registration requirement specifying the purpose of direct mailing and specific recordkeeping requirements. Moreover, the IPA Guidelines No. 2/2017 impose additional requirements intended for direct mailing services, which, *inter alia*, include specific notice obligations such as indication of database information, sources and an initial opt-in requirement.

Additionally, the said IPA Guidelines govern direct marketing services which, inter alia, require specific opt-in consents and notice requirements.

In 2020, the Knesset approved Amendment 61 to the Consumer Protection Law, 5571-1981 ("Consumer Protection Law") which proposed to establish an opt-out arrangement for telephone marketing calls, known as "Do not call me" database, so that such calls could be held unless a consumer refused through active registration in the database. Consumers are able to register their phone numbers in the "Do Not Call Me" database from December 12, 2022.

ONLINE PRIVACY

The PPL does not specifically address online privacy, cookies and / or location data, all of which are governed by the general restrictions detailed above, including the requirements imposed on processing databases and direct marketing and the consent, purpose and proportionality restrictions.

The PPL governs information "about a person", as such depending upon the circumstances at hand, any nonidentifiable and anonymous information (which cannot be reidentified) may reasonably be interpreted as falling outside the confines of the PPL limitations.

KEY CONTACTS

Goldfarb Seligman & Co., Law Offices
www.goldfarb.com

Sharon Aloni
Partner
Goldfarb Seligman & Co., Law Offices
T +972 (3) 608 9834
sharon.aloni@goldfarb.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ITALY

Last modified 19 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Italian data protection law framework has been harmonized with the GDPR by means of the Legislative Decree 101 /2018, that entered into force on 19 September 2018, and amended a number of provisions of the Legislative Decree 196 /2003 (the "**Privacy Code**"), as well as introduced some transitional provisions regulating the migration to the new regime.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor " *processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Italian Privacy Code adopts the definitions provided by the GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Privacy Code provides that the supervisory authority in Italy is the Garante per la protezione dei dati personali (the “**Garante**”). The Garante is composed of a Council and an Office. The Council is made up of four members, two elected by the Chamber of Deputies and two by the Senate of the Republic. The members are elected amongst those who apply for this position in a selection procedure whose details are published on the websites of the Chamber of the Deputies, the Senate of the Republic and the Garante. The members elect a Chairman, in the event of parity of votes. Law Decree 139/2021 (so-called “Decreto Capienze”) introduced an important change to the number of Garante’s members, which, starting from January 1st, 2022, increases from 162 to 200 members, recruited by way of a public competition.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of

personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Under the GDPR and the Privacy Code there is no obligation to notify regulators of any data processing activity.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organisations must not only comply with the GDPR but also be able to demonstrate compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;

- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data – i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose;
- the context in which the data have been collected;
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible);
- the possible consequences of the new processing for the data subjects;
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;

- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

- necessary for entering into or performing a contract;
- authorised by EU or Member State law; or
- the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Data Act

The Regulation on harmonized rules on fair access to and use of data (Data Act) has been approved on January 11th 2024. This regulation puts obligations on manufacturers and service providers to let their users, both companies and individuals, access and reuse data generated by the use of their products or services and share such data to third parties. It also improves data portability in all economic sectors.

Article 2-*ter* of the Privacy Code (as amended by Law Decree 139/2021) provides that, in case of processing of personal data for reasons of public interest or in connection with the exercise of public powers, the legal basis may also derive from a general administrative act. In such cases where it is necessary to disseminate or communicate personal data to other subjects for reasons of public interest or in connection with the exercise of public powers, it will be required to notify the Garante at least 10 days before the start of the communication or dissemination.

Furthermore, since Law Decree 139/2021 repealed Article 2-*quinquiesdecies*, the Garante is no longer entitled to prescribe the data controller to adopt measures and precautions to safeguard the data subjects for data processing that pose a high risk for the same, in case of processing of personal data performed for reasons of public interest or in connection with the exercise of public powers.

Article 2-*sexies* of the Privacy Code specifies that the processing of special category data necessary for the performance of a task carried out in the public interest is allowed insofar as the processing is provided for by European or domestic legislation, or, as recently introduced by the Law Decree 139/2021, by a general administrative act. This legislation must identify the reasons of public interest for which the processing is carried out, the types of data that can be processed, the operations that can be performed and the appropriate and specific measures protecting the fundamental rights and interests of the data subjects. In this context, the Privacy Code underlines that processing of genetic data, biometric data or data concerning health shall comply with additional requirements to be identified by the Garante by means of specific measures establishing further conditions in which the data processing is permitted.

With regard to personal data relating to criminal convictions and offences, Article 2-*octies* of the Privacy Code provides that the processing can be carried out only if a specific legal provision authorizes the processing, also identifying the applicable security measures, otherwise processing activities have to be carried out under the control of a public authority.

With regard to individuals’ rights, Art. 2-*undecies* of the Privacy Code provides several restrictions on data subjects’ rights for reasons of justice. In particular, data subjects rights may be exercised within the limits established in the law and regulations on the proceeding and procedures before the courts. The exercise of such rights may be delayed, limited or excluded for as long as and to the extent that it is a necessary and proportionate measure, having regard to the fundamental rights and legitimate interests of the data subject. Finally, the Privacy Code sets out data protection rights of deceased persons. Indeed, the rights provided for in Articles 15 through 22 of the GDPR referring to personal data concerning deceased persons may be exercised by those having an interest of their own, or act to protect the data subject, as her / his delegate, or for family reasons worthy of protection. The exercise of such rights is not permitted when provided for by the law or when, specifically limited to the offer of information society services, the data subject expressly prohibited it in writing by way of a declaration sent to the data controller. The data subject may withdraw or modify such declaration at any time.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

On July 10, 2023, the EU Commission adopted an adequacy decision pursuant to art. 45 of the GDPR. In its adequacy decision, the Commission has carefully assessed the requirements that follow from the EU-U.S. Data Privacy Framework ("DPF") and has decided that the United States ensures an adequate level of protection for personal data transferred from the EU to companies participating in the DPF.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU - U.S. Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

- explicit informed consent has been obtained;
- the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
- the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The Privacy Code does not derogate from the GDPR in regard to transfers.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The Privacy Code does not prescript further security measures that should be followed to protect personal data.

Nevertheless, genetic data, biometric data or data concerning health must be processed in accordance with the additional safeguard measures issued by the Garante every two years (Article 2-*septies*). Such safeguard measures take into account the guidelines, recommendations and best practices published by the European Data Protection Board and best practices on personal data processing; scientific and technological evolution in the sector covered by such measures; and the interest of the free flow of personal data within the territory of the Union. Also, the Garante may issue codes of ethics that set out security measures for the processing of personal for statistical and scientific research purposes.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

In the new version of the European Data Protection Board Guidelines 09/2022 issued on March 28, 2023, the EDPB specified the mere presence of a representative of a data controller not established in the EU does not trigger the one-stop-shop system. Therefore, the data breach shall be notified to every supervisory authority for which affected data subjects reside in their Member State.

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Privacy Code does not set out additional rules on data breach notifications.

However, data breaches that require notification should be notified to the Garante by completing a form available at the Garante website. The notification form, once completed with the required information, must be sent via certified e-mail to the Garante and must be signed digitally (with qualified electronic signature / digital signature) or with handwritten signature.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The Privacy Code provides that investigations and enforcement actions handled by the Garante.

ELECTRONIC MARKETING

The GDPR and the Privacy Code apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). As further analyzed below, under Section 130 of the Privacy Code, the legal basis for electronic marketing is consent. The strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Privacy Code (Section 130) does not prohibit the use of personal data for the purpose of electronic marketing, but it requires the prior informed consent (opt-in) from the recipient of the communication. The use of automated calling or communications systems without human intervention for the purposes of direct marketing or for sending advertising materials, or else for carrying out market surveys or interactive business communication, as well as electronic communications performed by e-mail, facsimile, MMS or SMS-type messages or other means shall only be allowed with the contracting party’s or user’s consent. Such consent shall be recorded with reference to its date and the person giving it in order to be used as evidence of the consent.

Separate consents shall be required for the registration to a website and the opt-in to the delivery of marketing communications, however the data subjects may be required to provide a unique marketing consent covering the different marketing practices (e.g. marketing via SMS, email, telephone, market surveys, etc.) performed through the collected data, provided that such practices are outlined in the information notice provided to data subjects.

An additional separate consent shall be required for the transfer of collected personal data to third parties for marketing purposes. Said third party shall also be identified at least on the basis of its category of operation and provide an information notice to data subjects before the delivery of marketing communications.

Where a data controller uses, for direct marketing of his own products or services, electronic contact details for electronic mail supplied by a data subject in the context of the sale of a product or service, said data controller may fail to request the data subject’s consent, on condition that the services are similar to those that have been the subject of the sale and the data subject, after being adequately informed, does not object to said use either initially or in connection with subsequent communications. The data subject shall be informed of the possibility to object to the processing at any time, using simple means and free of charge, both at the time of collecting the data and when sending any communications for the purposes here referred.

Electronic marketing communications shall clearly identify the sender and provide to the recipient all necessary information in order for him / her to eventually refuse the delivery of the direct marketing material (*opt-out*).

The possibility for the recipient to opt-out from marketing communication services must be guaranteed both during the first contact with the recipient and during any following communications.

Marketing communications by way of non-automated telephone calls are permitted provided that either:

- the data subject has given his prior consent, if there is an ongoing relationship that has not expired for more than 30 days; or
- the number (that can now also be a mobile number) of the data subject is included in the telephone directory and (s)he has not entered in a public opt-out register ("*Registro delle Opposizioni*") and opted out from being contacted for marketing purposes.

Law 11 January 2018, no. 5 provides stringent rules on telemarketing, including, amongst others, the withdrawal from all consents previously given in case of enrolment in the *Registro delle Opposizioni*, save for consents provided based on contractual arrangements in place or expired less than 30 days before the enrolment, and the prohibition to communicate, transfer or disseminate personal data related to data subjects registered in the *Registro delle Opposizioni* for advertising or sales purposes or for the purposes of carrying out market research or commercial communications not related to the activities, products or services offered by the data controller.

On March 24, 2023 the Garante approved a Code of Conduct for telemarketing and teleselling activities (*Codice di condotta per le attività di telemarketing e teleselling*), which is a self-governance instrument that contributes to the correct application of telemarketing regulations and to the dissemination of consumer protection principles and measures among call centres and other operators in the sector. This Code of Conduct applies to all operators that carry out activities of promotion and / or offer of goods and services by telephone to persons on Italian territory that can adhere to it on a voluntary basis. The Code of Conduct envisages several obligations - not strictly related to personal data protection – to which those engaged in telemarketing / teleselling activities must comply with, such as (i) register with the Register of Communications Operators ("**ROC**") and use only the numbers registered with the ROC; (ii) notify the Italian Ministry of Economic Development, Ministry of Labor, National Labor Inspectorate and the Italian Data Protection Authority in case of relocation to a non-EU country (and inform the user at the beginning of the call); and (iii) present the calling line using an appropriate prefix code (or using a number without a code as long as it is registered with the ROC and can be redialed).

The above mentioned privacy provisions apply also to communications sent through private messages on social networks and through *Voip*. On the contrary, should the data subject be a follower of a social network page, it may be implied that the data subject has consented to the delivery of marketing communications of the page. Marketing messages concerning a given brand, product or service as sent by the company managing the relevant social network page may be considered to be lawful if it can be inferred unambiguously from the context or the operational arrangements of the relevant social network, also based on the information provided, that the recipient did intend in this manner to also signify his / her intention to consent to receiving marketing messages from the given company. However the delivery of marketing communications shall stop when the data subject unregisters from the page.

The Privacy Code provisions relating to marketing and commercial communications make reference to the ‘contracting party’s and user’s consent’ rather than to the ‘data subject’s consent’, referring both to individuals and companies.

ONLINE PRIVACY

The Privacy Code regulates the collection and processing of traffic data and location data by the provider of a public communications network or publicly available electronic communications service and the use of cookies.

According to Section 123 of the Privacy Code, traffic data shall be erased or made anonymous when they are no longer necessary for the purpose of transmitting the electronic communication. However traffic data can be retained for a period not longer than 6 months for billing and interconnection payments purposes or, with the prior consent of the contracting party or user (which may be withdrawn at any time), for marketing electronic communications services or for the provision of value added services.

According to Section 126 of the Privacy Code, location data may only be processed if made anonymous or if the subscriber or user has been properly informed and (s)he has given her / his prior consent (which can be withdrawn at any time).

According to Section 122 of the Privacy Code (which reflects recital 66 of the E-Cookies Directive 2009/136/EC and the amended Section 5, par. 3 of the Directive 2002/58/EC – as amended by Directive 2009/136/EC) the storing of information in the contracting party’s or user’s computer is only allowed if said contracting party or user has been properly informed and (s)he has given her / his consent.

In July 2021, the Garante released a new set of guidelines for the use of cookies and other tracking tools which introduce a number of new provisions (“**New Cookie Guidelines**”). Companies had to comply to the new rules, starting from January 9, 2022. Among other things, the New Cookie Guidelines provide that:

- as a general rule, scrolling or swiping a page is not considered a valid mechanism to collect the user’s consent, unless it can be proved that scrolling or swiping of the user is the result of an unequivocal choice;
- the request of consent to cookies may not be resubmitted to the user, unless (i) the conditions for processing of personal data significantly change, (ii) it is not possible for the operator of the site to record the previous choice of the user due to a decision of the latter (e.g. deletion of cookies) and (iii) at least 6 months have expired since the previous request;
- the user must be able to continue browsing without being tracked by cookies and he / she must be able to withdraw his / her consent at any time.

With specific reference to the configuration of the cookie banner, the Garante provides that the same shall contain the following elements:

- a command (e.g. an “X” at the top right corner of the cookie banner) which allows the user to close the banner while keeping the default settings and therefore not to give consent to the storing of cookies or the use of other profiling techniques or a command indicating that users continue the navigation of the site without accepting cookie;
- a command to accept all cookies or other tracking tools;
- a short notice on the website’s use of technical cookies and any profiling cookies or other tracking tools, with the relevant purposes;
- a link to the extended cookie policy which indicates any other recipients of personal data, the data retention period and the rights of users; and
- a link to a dedicated area where users can choose, in a granular way, the cookies to be installed with regards to their functionalities, third parties and categories.

Furthermore, the New Cookie Guidelines clarify that a cookie information notice shall be provided:

- in an accessible and simple language;
- which is easily accessible, without discriminations, also to those individuals with disabilities which require them to use assistive technologies and particular configurations;

- also in a multi-layer and multi-channel modality;
- which can be inserted with the website homepage or general privacy information notice, insofar as the website installs technical cookies only; and
- which categorizes cookies and other tracking tools so as to enable distinguishing between technical cookies, analytics cookies and profiling cookies, using a clear, concise and transparent language and layout, insofar as the website installs other categories of cookies than the technical ones.

KEY CONTACTS

Giulio Coraggio
Partner
T +39 02 80 6181
giulio.coraggio@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

JAPAN

Last modified 1 January 2024

LAW

The Act on the Protection of Personal Information ("**APPI**") regulates privacy protection issues in Japan and the Personal Information Protection Commission ("**PPC**"), a central agency acts as a supervisory governmental organization on issues of privacy protection.

The APPI was originally enacted in 2003 but was amended and the amendments came into force on 30 May 2017. On 5 June 2020, the Japanese Diet approved a bill to further amend the APPI ("**Amended APPI**"). The Amended APPI came into force on April 1, 2022. Also, there was a separate data protection law for public sector. However, the data protection law for public sector was integrated into the APPI and became effective on April 1, 2022 (the data protection law for local governments became effective after April 1, 2023).

DEFINITIONS

Definition of Personal Information

Personal Information is information about a living individual which can identify a specific individual by name, date of birth or other description contained in such information. Personal Information includes information which enables one to identify a specific individual with easy reference to other information. According to the guidelines issued by the PPC, "easy reference to other information" means that a business operator can easily reference other information by a method taken in the ordinary course of business. If a business operator needs to make an inquiry of another business operator to obtain the "other information" and it is difficult for the business operator to do so, such a situation would not be considered an "easy reference to other information".

Personal Information includes any "Personal Identifier Code". A Personal Identifier Code refers to certain types of data specified under a relevant cabinet order of the APPI, and includes biometric data which can identify a specific individual, or data in the form of a certain code uniquely assigned to an individual. Typical examples of such code would be passport numbers or driver's license numbers.

Definition of Sensitive Personal Information

Sensitive information includes information about a person's race, creed, social status, medical history, criminal record, any crimes a person has been a victim of, and any other information that might cause the person to be discriminated against. Obtaining sensitive information generally requires consent from the data subject. Additionally, the "opt out" option (discussed below) is not available for third party transfer for sensitive information-prior consent is basically required from the data subject to transfer the sensitive information to a third party.

Definition of Anonymously Processed Information

"Anonymously Processed Information" refers to any information about individuals from which all personal information (i.e. the information that can identify a specific individual, including any sensitive information) has been removed and such removed personal information cannot be restored by taking appropriate measures specified in the enforcement rules and the relevant PPC guidelines. As noted above, Personal Information includes personal identifier codes, so these must also be removed before information is considered anonymized.

If a business operator has sufficiently anonymized the information, it can be used beyond the purpose of use notified to the data subjects or disclosed to third parties without requiring the consent of the data subjects. However, care must be taken in anonymizing the information before disclosure; a failure to completely sanitize the information could result in the disclosure of Personal Information. Additionally, before disclosing the Anonymously Processed Information to a third party, a business operator must publicly state (likely in its privacy policy) the items of information (for example, gender, birth year and purchase history) included among the Anonymously Processed Information, and the means by which it shares the Anonymously Processed Information.

Definition of Pseudonymously Processed Information

Given the high hurdle of utilizing Anonymously Processed Information, such information has been less utilized than originally expected. The Amended APPI introduces the concept of "Pseudonymously Processed Information", which is the information that is processed so that such information is (i) not able to be used to identify a specific individual; but (ii) is able to be de-crypted by referencing other information. For example, Pseudonymously Processed Information is information in which names, addresses, and other similar such information are replaced with a random string of characters. Unlike normal Personal Information, a business operator can change the utilization purpose of Pseudonymously Processed Information at its own discretion (i.e. a business operator does not need to obtain consents from data subjects to change the utilization purpose). It is expected that business operators may utilize Pseudonymously Processed Information for internal data analytics purposes.

Definition of Personally Referable Information

The Amended APPI defines information which is related to personal matters, but that does not fall under the definition of Personal Information as "Personally Referable Information". The definition of Personally Referable Information is quite vague, but based on the guidelines issued by the PPC, it includes, among other things, a web browsing history collected through the terminal identifier such as cookie information, a person’s age, gender or family makeup that are linked to his / her email address, a person’s purchase history of goods and / or services, a person’s location data, or a person’s area of interest. The handling of Personally Referable Information is not regulated as Personal Information, but prior consent from data subjects would be required to transfer Personally Referable Information in certain circumstances as discussed below.

NATIONAL DATA PROTECTION AUTHORITY

The PPC has been tasked with providing many of the details necessary to interpret and enforce the APPI. The PPC issues guidelines for general rules for handling Personal Information, offshore transfer, confirmation and record requirements upon provision of Personal Information to third parties and creation and handling Anonymously or Pseudonymously Processed Information. The PPC is neutral and independent, and it has the power to enforce the APPI. However, it will only have the right to perform audits and issue cease and desist orders; it will not have the power to impose administrative fines and criminal penalties.

Personal Information Protection Commission

Kasumigaseki Common Gate West Tower
32nd Floor
3-2-1 Kasumigaseki
Chiyoda-ku Tokyo 100-0013
Japan

Telephone

+81-(0)3-6457-9680

Website

ppc.go.jp

REGISTRATION

Japan does not have a central registration system.

DATA PROTECTION OFFICERS

There is no specific legal requirement to appoint a data protection officer. However, some guidelines provide that specific directors or employees should be assigned to control Personal Information (e.g. Chief Privacy Officer).

COLLECTION & PROCESSING

Specifying the Purpose of Use

When handling Personal Information, a business operator must specify to the fullest extent possible the purpose of use of the Personal Information ("Purpose of Use"). Once a business operator has specified the Purpose of Use, it must not then make any changes to the said purpose which could reasonably be considered to be beyond the scope of what is duly related to the original Purpose of Use. In addition, when handling Personal Information, a business operator shall not handle the information beyond the scope that is necessary for the achievement of the Purpose of Use without a prior consent of the individual. In other words, the use of the information must be consistent with the stated Purpose of Use.

Public Announcement of the Purpose of Use

The Purpose of Use must be made known to the data subjects when Personal Information is collected or promptly thereafter and this can be made by a public announcement (such as posting the purpose on the business operator's website). When Personal Information is obtained by way of a written contract or other document (including a record made in an electronic or magnetic format, or any other method not recognizable to human senses), the business operator must expressly state the Purpose of Use prior to the collection.

A business operator must 'publicly announce or 'expressly show the Purpose of Use in a reasonable and appropriate way. According to the guidelines issued by the PPC, the appropriate method for a website to publicly announce the Purpose of Use of information collected, is a one click access on the homepage so that the data subject can easily find the Purpose of Use before submitting the Personal Information.

TRANSFER

Disclosing / Sharing Personal Information

Currently, Personal Data (meaning Personal Information stored in a database) may not be disclosed to a third party without the prior consent of the individual, unless the business operator handling the Personal Information adopts the opt-out method, provides an advance notice of joint use to data subjects, in the case of merger / business transfer or entrusting the handling of Personal Information to third party service providers.

Even disclosing the Personal Information within group companies is considered disclosing the Personal Information to a third party and consent must be obtained, unless it meets the requirements of joint use. The APPI also has permitted the "opt out" method, whereby a business operator can as a default disclose Personal Information to third parties, unless individuals opt out of allowing the business operator to do so. The Amended APPI stipulates that Personal Information that has been transferred from others through the opt out measure or that has obtained by illegal manners, and Sensitive Personal Information cannot be transferred through the opt out measure. The APPI requires a business operator to preemptively disclose to the PPC, and the public or to the data subject of certain items listed below concerning opt out.

- the name, address and representative person of the business operator;
- the fact that the purpose of use includes the provision of such information to third parties;
- the nature of the Personal Information being provided to third parties;
- the method by which Personal Information has been obtained;
- the method by which Personal Information will be provided to third parties;
- the matter that provision of such information to third parties will be stopped upon the request by the data subject;
- the method for an individual to submit an opt out request to the business operator;
- the method to update Personal Information which has been provided to their parties; and
- the schedule date of provision of Personal Information.

The APPI does not provide any examples of how best to obtain consent from individuals before sharing Personal Information. Generally, written consent should be obtained whenever possible. When obtaining consents, it would be prudent to clearly disclose to the data subject the identity of the third party to whom the Personal Information will be disclosed, the contents of the Personal Information and how the third party will use the provided Personal Information.

The guidelines issued by the PPC provide the following examples as appropriate methods of obtaining the consent for disclosing Personal Information from the data subject:

- receipt of confirmation of the oral or written consent (including a record created by electronically or magnetically methods or any other method not recognizable to human senses) from data subject;
- receipt of a consent email from data subjects;
- the data subject's check of the confirmation box concerning the consent;
- the data subject's click of a button on the website concerning the consent; and
- the data subject's audio input, or touch of a touch panel concerning the consents.

If Personal Information is to be used jointly, the business operator could, prior to the joint use, notify the data subjects of or publish the following:

- the fact that the Personal Information will be used jointly;
- the item of the Personal Information to be disclosed;
- the scope of the joint users;
- the purpose for which the Personal Information will be used by them; and
- the name, address and representative person of the business operator responsible for the management of the Personal Information.

Transfer of Personally Referable Information

The Amended APPI stipulates that prior consent from data subjects is necessary if Personally Referable Information is transferred to a third party and the receiving party can identify a specific individual by way of referencing such Personally Referable Information with any information that the receiving party already has in its possession. In general, such consents are to be obtained by the receiving party and therefore, the transferor needs to, in advance to transferring Personally Referable Information to a third party, confirm if the receiving party has already obtained consents. That being said, it is possible that the transferor collects data subjects’ consents on behalf of the receiving party.

Cross-border Transfer

Under the APPI, in addition to the general requirements for third party transfer, prior consent of data subjects specifying the receiving country is required for transfers to third parties in foreign countries unless the foreign country is white-listed under the

enforcement rules of the APPI or the third party receiving Personal Information has established similarly adequate standards for privacy protection as specified in the enforcement rules of the APPI. Currently, UK and EU countries are specified as white-listed countries based on the adequacy decision on January 23, 2019.

According to the enforcement rules of the APPI, "similarly adequate standards" means that the practices of the business operator handling the Personal Information are at least equal with the requirements for protection of Personal Information under the APPI or that the business operator has obtained recognition based on international frameworks concerning the handling of Personal Information.

According to the guidelines for offshore transfer, one of the examples of an acceptable international framework is the APEC CBPR system. With regard to data subject's consents to transfer their Personal Information to foreign countries, the Amended APPI stipulates that the business operator shall provide the following information to the data subject when obtaining consents therefrom: (i) name of the country where the receiving party resides, (ii) data protection law system in the country and (iii) the data protection measures that the receiving party implements. In addition, the business operator needs to take necessary measures to ensure that the receiving party of such Personal Information continuously takes proper measures to process the Personal Information in a manners equivalent to the requirements of the APPI.

SECURITY

The APPI requires that business operators prevent the leakage of Personal Information. The APPI does not set forth specific steps that must be taken. The PPC guidelines suggest recommended steps that business operators should take to ensure that Personal Information is secure. These necessary and appropriate measures generally include "Systematic Security Control Measures", "Human Security Control Measures", "Physical Security Measures" and "Technical Security Control Measures".

Guidelines often contain several specific steps or examples that entities subject to the guidelines must take with respect to each of the security control measures such as developing internal guidelines pertaining to security measures, executing non-disclosure contracts with employees who have access to Personal Information, protecting machines and devices and developing a framework to respond to instances of leakage.

BREACH NOTIFICATION

Under the Amended APPI, business operators shall report data breach incidents to the PPC and affected data subjects if the data breach incidents could harm the rights and interests of individuals. The PPC set the concrete threshold for reporting obligations and in the case of any of the below (i)-(iv), the business operator needs to report it to the PPC and notify the affected individuals: (i) Sensitive Personal Information is or likely to have been leaked, (ii) Personal Information that would cause financial damage by unauthorized use is or likely to have been leaked, (iii) data leakage by wrongful purpose is or likely to have been occurred, and (iv) data leakage incident that involves more than 1,000 data subjects is or likely to have been occurred.

In addition, the PPC guidelines suggest that business operators (i) make necessary investigations and take any necessary preventive measures, and / or (ii) make public the nature of the breach and steps taken to rectify the problem, if appropriate and necessary.

According to the PPC guidelines, if a factual situation demonstrates that the Personal Information which has been disclosed was immediately collected before being seen by any third party or not actually disclosed, (such as the case where the company has encrypted the data or otherwise secured the data in such a way that it has become useless to third parties being in possession of such data), the notice to the PPC or any other relevant authority is not necessary.

ENFORCEMENT

If the PPC finds any violation or potential violation of the APPI, the PPC may request the business operator to submit a report, conduct on-site inspection and request or order the business operator to take remedial actions. If a business operator does not submit the report and materials, or reports false information they will be subject to a fine of up to JPY 500,000.

If a business operator does not follow an order from the PPC they will be subject to a penalty of imprisonment for up to one year or a fine of up to JPY 1,000,000. If the party that fails to follow such order is an entity, the parties subject to this penalty will

be the relevant officers, representatives, or managers responsible for the disclosure and the entity is subject to the fine of up to JPY 100,000,000.

An unauthorized disclosure of Personal Information, for the benefit of the disclosing party or any third party, will be subject to a penalty of imprisonment for up to one year or a fine of up to JPY 500,000. If the party that discloses Personal Information is an entity, the parties subject to this penalty will be the relevant officers, representatives, or managers responsible for the disclosure and the entity is subject to the fine of up to JPY 100,000,000.

ELECTRONIC MARKETING

The Act on Specified Commercial Transactions ("**ASCT**") and the Act on the Regulation of Transmission of Specified Electronic Mail ("**Anti-Spam Act**") regulate the sending of unsolicited electronic commercial communications.

Under the ASCT, which focuses on internet-order services, a seller is prohibited from sending email or fax advertisements to consumers unless they provide a prior request or consent (i.e. an opt-in requirement). The seller is also required to retain the records that show consumers' requests or consents to receive email or fax advertisements for 3 years for email advertisements and 1 year for fax advertisements after the last transmission date of an email or fax advertisement to the consumer.

If a seller has breached any of these obligations regarding email advertisements, such seller will be potentially subject to fine of up to JPY 1,000,000.

Under the Anti-Spam Act, which broadly covers commercial emails (e.g. an invitation email from a social network service), there are several regulations on sending email advertisements as follows:

- the sender must retain records evidencing there was a request or consent to receive emails at least for 1 month after the last date the seller sent an email to the recipient;
- for-profit entities or individuals engaged in business sending any email to advertise their own or another’s business must obtain a request or consent to receive emails from intended recipients unless the recipient falls under certain exceptions (e.g. there is a continuous transaction relationship between a sender and a recipient) in the Anti-Spam Act;
- an email is required to include a sender’s email address or a URL so that recipients can send opt-out notices to the sender; and
- senders must not send emails to randomly generated email addresses (with the hope of hitting an actual email address) for the purpose of sending emails to a large number of recipients.

The relevant ministry may order a sender to improve the manner of email distribution if the sender violates the requirements noted above. If the sender violates an order issued by the ministry (other than one related to the retention obligation), the sender is subject to imprisonment for up to 1 year or a fine of up to JPY 1,000,000. In addition, the entity will be subject to fine of up to JPY 30,000,000 if an officer or an employee of the entity commits any violation mentioned above. If the sender violates an order issued by the minister with respect to the retention obligation, the sender will be potentially subject to fine of up to JPY 1,000,000. In addition, the entity will be subject to fine of up to JPY 1,000,000 if an officer or an employee of the entity commits the violation mentioned above.

ONLINE PRIVACY

There is no law in Japan that specifically addresses cookies, but it is generally considered that cookies fall under the definition of the Personally Referable Information and thus the transfer of such data would be regulated by the APPI in certain circumstances. In addition, if the information obtained through cookies may identify a certain individual in conjunction with other easily-referenced information (e.g. member registration) and it is utilized (e.g. for marketing purposes), such Purpose of Use of information obtained through the use of cookies must be disclosed under the **APPI**.

Moreover, under the Telecommunications Business Act, when providing telecommunications services to users as specified in the applicable Ministry of Internal Affairs and Communications ordinance and sending a telecommunication to the user’s device that gives a command to activate the device's information transmission function which transfers the information to third parties (such as third-party cookie), the service provider must take one of the following measures: (i) notify users of the content of information to be sent, Purpose of Use and the destination of information to be sent, or put these information in a condition where users can easily learn about it, (ii) obtain users consent, or (iii) take opt-out measures.

KEY CONTACTS

Tomomi Fujikouge
Of Counsel
T +81 3 4550 2817
tomomi.fujikouge@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

JERSEY

Last modified 11 January 2024

LAW

The Data Protection (Jersey) Law, 2018 (DPJL) and the Data Protection Authority (Jersey) Law, 2018 (DPAJL) came into force on May 25, 2018. These laws superseded the Data Protection (Jersey) Law 2005, which had been held to be adequate by the European Commission for the purposes of the European Data Protection Directive (Directive 95/46/EC) (see Commission Decision 2008/393/EC). This decision continues to apply pending a review of Jersey's adequacy (to be conducted under Article 45 of the European General Data Protection Regulation (GDPR)), the outcome of which was expected in 2021 but is now expected during 2023.

The DPJL and DPAJL provide a broadly equivalent regime to that under the GDPR.

DEFINITIONS

The DPJL defines 'data' as information that:

- Is processed by means of equipment operating automatically in response to instructions given for that purpose or is recorded with the intention that it should be processed by means of such equipment
- Is recorded as part of a filing system or with the intention that it should form part of a filing system, or
- Is recorded information held by certain public authorities

The DPJL defines 'personal data' as being any data relating to a data subject.

A 'data subject' is defined in the DPJL as an identified or identifiable, natural living person who can be identified, directly or indirectly, by reference to (but not limited to) an identifier such as:

- A name, an identification number or location data
- An online identifier (which may include an IP address, location data or any unique number or code issued to the individual by a public authority), or
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the person

Enhanced levels of protection in the DPJL and DPAJL are provided for 'special category' personal data.

'Special category personal data' is defined under the DPJL as personal :

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership
- Genetic or biometric data that is processed for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person’s sex life or sexual orientation, or
- Data relating to a natural person’s criminal record or alleged criminal activity

Personal data may be processed by either a **'controller'** or a **'processor'**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 1(1) DPJL). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the DPJL imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

NATIONAL DATA PROTECTION AUTHORITY

The DPAJL created a Data Protection Authority (the Authority) to oversee the DPJL. Save in respect of certain matters (in particular the issuing of a formal public statement in relation to data protection issues or the issuing of an administrative fine), its functions are delegated to the Information Commissioner.

REGISTRATION

Registration and fees are governed by the Data Protection (Registration and Charges) (Jersey) Regulations 2018 (as amended) (the "**Regulations**") under which annual processing fees are charged, the value of which are based on:

- the number of full-time employees;
- the level of past-year revenue;
- whether the relevant entity is a regulated financial services provider (or otherwise subject to the Money Laundering (Jersey) Order 2008);
- if the entity processes special category data; and
- if the entity is administered by a trust company business or fund services business, and if so, the name of the administrator.

The maximum fee payable on the basis of the above is £1,600. However, the majority of data controllers and processors pay £70.

Entities that are administered by a regulated trust company business or fund services business are required to pay a fixed annual charge of £50. No fees are payable where the entity does not process data (as they would not be considered data controllers or processors).

All controllers and processors are required to renew their registration annually. It should be noted that, external accountability to the Information Commissioner via registration or notification has in many ways superseded in the DPAJL and DPJL by rigorous demands for internal accountability.

In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 14(3) DPJL), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request.

DATA PROTECTION OFFICERS

Data controllers and processors are required (Article 24 DPJL) to appoint a data protection officer if:

- Processing is carried out by a public authority (with the exception of courts acting in their judicial capacity)
- The core activities of the controller or the processor consist of processing operations that, by virtue of their nature, scope or purposes, require regular and systematic monitoring of data subjects on a large scale
- The core activities of the controller or the processor consist of processing special category data on a large scale, or
- It is otherwise required by law

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 24(3) DPJL). However, larger corporate groups may find it difficult in practice to operate with a single data protection officer. The data protection officer must be easily accessible to:

- All data subjects
- The Information Commissioner, and

- The controller or processor who appointed the officer, along with the controller’s or processor’s employees that carry out data processing

Data protection officers (DPOs) must have expert knowledge (Article 24(6) DPJL) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 24(7) DPJL).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 25(1) DPJL), and the DPO must directly report to the highest management level of the controller or processor (Article 25(2) DPJL).

In addition, controllers and processers must:

- Ensure that the data protection officer operates independently and does not receive any instructions regarding the performance of those duties, other than to perform them to the best of the officer’s ability and in a professional and competent manner (Article 25(1)(c) DPJL), and
- Not dismiss or penalize the data protection officer for performing his or her duties other than for failing to perform them to the best of the officer's ability and in a professional and competent manner (Article 25(1)(d) DPJL)

The specific tasks of the DPO are set out in Article 26 DPJL and include:

- Informing and advising on compliance with the DPJL, DPAJL and other applicable data protection laws
- Monitoring compliance with the law and with the internal policies of the organization, including assigning responsibilities, raising awareness and training staff
- Advising on and monitoring data protection impact assessments, where requested, and
- Cooperating and acting as point of contact with the Information Commissioner

COLLECTION & PROCESSING

Controllers are responsible for compliance with a set of core principles that apply to all processing of personal data. Under these principles, personal data must be (Article 8(1) DPJL):

- Processed lawfully, fairly and in a transparent manner in relation to the data (‘lawfulness, fairness and transparency’)
- Collected for specified, explicit and legitimate purposes and once collected, not further processed in a manner incompatible with those purposes (‘purpose limitation’)
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘ data minimization’)
- Accurate and, where necessary, kept up-to-date, with reasonable steps being taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘ accuracy’)
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed (‘storage limitation’) and
- Processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’)

Additionally, the controller is responsible for and must be able to demonstrate compliance with the above principles (‘ accountability’) (Article 6(1)(a) DPJL).

Accountability is a core theme of the DPJL. Organizations must not only comply with the DPJL, but also be able to *demonstrate* compliance, perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving (and being able to demonstrate) accountability.

Legal Basis for Processing

The DPJL works slightly differently to the GDPR in terms of establishing a legal basis for processing.

Data controllers may collect and process personal data when any of a number of conditions are met (Article 9 and Schedule 2 DPJL). The most frequently relied upon are as follows:

- The consent of the data subject
- The processing is necessary for:
  - The performance of a contract to which the data subject is a party, or
  - The taking of steps at the request of the data subject with a view to entering into a contract
- The processing is necessary to comply with a data controller’s legal obligations (other than one imposed by contract)
- The processing is necessary to protect the data controller’s vital interests
- The processing is necessary for:
  - The administration of justice
  - The exercise of any functions conferred on any person by or under any enactment
  - The processing is necessary for taking legal advice or the establishment, exercise or defense of legal claims
  - The exercise of any functions of the Crown, the States or any public authority, or
  - The exercise of any other functions of a public nature with a legal basis in Jersey law to which the controller is subject and exercised in the public interest by any person
  - The processing is necessary for the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, unless:
    - The processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject, in particular where the subject is a child, or
    - The controller is a public authority, or
  - The processing is necessary for reasons of substantial public interest provided for by law and is subject to appropriate protections to protect the rights and interests of the data subject

Special Categories of Data

Where special category personal data is processed, at least one of a more restrictive list of conditions than those for personal data must be satisfied (Article 9 and Schedule 2 Part 2 DPJL). Unlike the GDPR, personal data may also be processed on the basis of the conditions for processing special category data. The most frequently relied upon bases for processing special category data are as follows:

- The explicit consent of the data subject
- The processing is necessary to comply with a data controller’s legal obligations (other than one imposed by contract)
- The processing is necessary for the purposes of exercising or performing any right, obligation or public function conferred or imposed by law on the controller in connection with employment, social security, social services or social care
- The processing is necessary for taking legal advice or the establishment, exercise or defense of legal claims
- The processing is necessary for reasons of substantial public interest provided for by law and is subject to appropriate protections to protect the rights and interests of the data subject
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- The processing relates to personal data which are manifestly made public by the data subject
- The processing is necessary for archiving or research
- The processing is necessary for the prevention of unlawful acts (or malpractice / mismanagement)
- The processing is necessary for certain insurance-based purposes, or
- The processing is necessary for medical purposes and is undertaken by a health professional

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data *(ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected). This is potentially in conflict with the core principle of purpose limitation, which aims to ensure that the rights of data subjects are protected. The DPJL sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 13 DPJL)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are, it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects, and
- The existence of appropriate safeguards

Transparency

The data controller must provide the data subject with “fair processing information” (Article 12 DPJL), which includes:

- The identity and contact details of the controller, and where applicable, the controller’s representative
- The contact details of the data protection officer (if any)
- The purposes for which the data are intended to be processed and the legal basis for the processing
- An explanation of the legitimate interests pursued by the controller or by a third party, if the processing is based on those interests
- The recipients or categories of recipients of the personal data (if any)
- Where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and whether or not there is an adequate level of protection for the rights and freedoms of data subjects in that country or organization
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- Information concerning the rights of data subjects
- Where the processing is based on consent, the existence of the right to withdraw consent
- The existence of any automated decision-making and any meaningful information about the logic involved in such decision-making and the significance of any such decision-making for the data subject
- A statement of the right to complain to the Information Commissioner
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failing to provide such data
- Where the personal data are not obtained directly from the data subject, information identifying the source of the data
- Any further information that is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in limited circumstances. Controllers must provide information on action taken in response to requests within four weeks as a default, with a limited right for the controller to extend this period a further eight weeks where the request is onerous. These periods are slightly shorter than those set out in the GDPR.

Right of access (Article 28 DPJL)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 31 DPJL)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 32 DPJL)

Data subjects may request erasure of their personal data.

The right is not absolute; it only arises in a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 33 DPJL)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed other than for legal claims of the data subject or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 34 DPJL)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format.

Right to object (Article 21 DPJL)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is for a public function. Controllers will then have to suspend processing of the data until such time as they demonstrate ‘compelling legitimate grounds’ for processing that override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time (Article 36 DPJL).

The right not to be subject to automated decision taking, including profiling (Article 38 DPJL)

Automated decision-making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

1. Necessary for entering into or performing a contract
2. Authorized by Jersey law or by the law of another jurisdiction in the British Isles or by EU or member state law, or
3. The data subject has given their explicit consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the controller must implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, including the right to obtain human intervention on the part of the controller, so that the data subject can express his or her point of view and contest the decision.

Children’s consent to information society services (Article 11(4))

Article 11(4) of the DPJL stipulates that a child may only provide his or her own consent to processing in respect of information society (primarily, online) services, where that child is over 13 years of age. Otherwise, a parent (or other responsible adult) must provide consent on the child’s behalf.

Processing agreements

The rules on agreements (or other legally binding instruments) between controllers and processors have been significantly enhanced.

The controller must appoint the processor in the form of a **binding written agreement** that sets out:

- The **subject matter** and **duration** of the processing
- The **nature** and **purpose** of the processing
- The **type of personal data** and **categories of data subjects**, and
- The obligations and rights of the controller

The agreement must also provide that the processor must:

- Only act on the controller's **documented** instructions (unless legally obliged to do otherwise)
- Impose **confidentiality obligations** on all **personnel** who process the relevant data
- Ensure the **security** of the personal data that it processes
- Abide by the rules regarding appointment of **sub-processors**
- Implement measures to assist the controller in complying with the rights of data subjects
- Assist the controller in:
    - Complying with its **data security obligations**
    - Complying with its **personal data breach** obligations (both to a supervisory authority and individual data subjects), and
    - Completing **Data Protection Impact Assessments** and **obtaining approvals from Supervisory Authorities** where required
- At the controller's election, either **return or destroy the personal data** at the end of the relationship (except as required by law), and
- Provide the controller with **all information necessary** to demonstrate compliance with the DPJL, which, in practice, means complying with an audit/inspection regime

TRANSFER

The DPJL (Article 67) provides that data controllers and processors may only transfer personal data out of the European Economic Area if one of the following conditions are met:

- The transfer is to a jurisdiction which has been held by the European Commission to provide an adequate level of protection for personal data.
- The transfer is made subject to ‘appropriate safeguards’ (Article 68 DPJL), which may include:
    - A legally binding and enforceable instrument between public authorities
    - Binding corporate rules approved by Jersey's Information Commissioner or another competent supervisory authority under the GDPR (or equivalent statutory provisions), or
    - Standard data protection clauses adopted by the Authority or by a competent supervisory authority and approved by the European Commission. It should be noted that the EDPB approved a new set of standard contractual clauses in June 2021, which have now been approved for use in Jersey (subject to also using a Jersey law addendum). It should be noted that the UK International Data Transfer Agreement has not yet been approved for use in Jersey.
- An exemption applies, the most commonly utilized of which are as follows:
    - The transfer is specifically required by a Jersey court
    - The data subject explicitly consents
    - The transfer is necessary for the performance of a contract to which the data subject is party or the implementation of pre-contractual measures taken at the data subject’s request
    - The transfer is necessary to carry out a contract between the data controller and a third party if the contract serves the data subject’s interests
    - The transfer:
        - Is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings)

        - Is necessary for the purpose of obtaining legal advice, or
        - Is otherwise necessary for the purposes of establishing, exercising or defending legal rights
    - The transfer protects the data subject’s vital interests where:
        - The data subject is physically or legally incapable of giving consent
        - The data subject has unreasonably withheld consent, or
        - The controller or processor cannot reasonably be expected to obtain the explicit consent of the data subject

Transfers post Schrems II

The burden on Jersey controllers and processors of transferring personal data to unauthorised jurisdictions has increased following the CJEU's Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited*, Maximillian Schrems and intervening parties ("**Schrems II**").

Following Schrems II, where Standard Contractual Clauses ("SCCs") are used, controllers (and where applicable processors) must ensure that they have considered their transfers and taken any steps appropriate to ensure that they are lawful.

However, the guidance does not provide any assistance as to what steps need to be taken in order to ensure that the chosen safeguards are appropriate. The required approach has since been clarified by the European Data Protection Board which published Recommendations 01/2020 in June 2021 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (see below). There is also local Jersey guidance which broadly tracks (and cross refers to) the EDPB guidance.

The emphasis is on controllers / processors to satisfy themselves that the transfers to unauthorised jurisdictions are properly assessed (taking into account the law and practice of the recipient jurisdiction) and, as appropriate, put in place supplementary measures.

CJEU jurisprudence is not binding in Jersey, as Jersey is not an EU member state. However, it is likely to be persuasive (as is the EDPB guidance noted above).

The EDPB guidance referenced above recommends a 6 step process in relation to international transfers.

1. **Know your transfers**. Be aware of where the personal data so you know the level of protection provided there. Make sure the data you transfer is adequate, relevant and limited to what is necessary.
2. **Verify** the transfer tool your transfer relies on.
3. **Assess** if there is anything in the law and / or practices of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer.
4. **Identify and adopt supplementary measures** necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence. This step is only necessary if your assessment has revealed issues with the third party country's safeguards. If no supplementary measure is suitable, the exporter must avoid, suspend or terminate the transfer.
5. **Take any formal procedural** steps the adoption of your supplementary measure may require.
6. **Re-evaluate at appropriate intervals** the level of protection afforded to the personal data you transfer to third countries and monitor if there have been or there will be any developments that may affect it. This is an ongoing duty.

In practice, the above requires a detailed and documented transfer impact assessment ("**TIA**").

Transfers between Jersey and the USA

The replacement of the Privacy Shield transfer scheme (invalidated by Schrems II) by the EU-US Privacy Data Privacy Framework means that Jersey controllers and processors are in principle able to utilise the new Framework for data transfers. However, the US Department of Commerce is yet to extend the scope of the Framework to cover Jersey and accordingly it is recommended that Jersey controllers and processors continue to utilise standard contractual clauses in respect of transfers between Jersey and the US.

What about the UK?

The European Commission has now recognised the UK as an adequate jurisdiction for the purposes of international data transfer and the UK has in turn recognised Jersey as an adequate jurisdiction for the purposes of the UK GDPR meaning that transfers to and from the UK and Jersey may continue without restriction.

Jersey controllers and processors who are subject to the UK GDPR by virtue of its extra territoriality provisions will also need to consider whether they may need to continue using the existing standard contractual clauses or the UK International Data Transfer Agreement.

SECURITY

Controllers and processors must implement technical and organizational measures against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data that are proportionate to the risk of harm posed to the rights of data subjects by such events (Article 21 DPJL).

'Technical measures' may include:

- The pseudonymization and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

BREACH NOTIFICATION

The DPJL includes obligations related to ‘personal data breaches’, which are defined in the DPJL as breaches of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data controllers must notify the Information Commissioner via an online portal (https://oicjersey.org/breach-reporting/) that a personal data breach has occurred within 72 hours of becoming aware of the breach (Article 20 DPJL). A breach does not need to be notified to the Information Commissioner where it is unlikely to result in a risk to the rights and freedoms of natural persons in respect of their personal data. If there is a high risk that the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the data controller must also notify those individuals.

Controllers are also required to keep a record of all data breaches (Article 20(5) DPJL) (whether or not notified to the Information Commissioner) and permit audits of the record by the Information Commissioner.

ENFORCEMENT

In Jersey, the Authority is responsible for the enforcement of the DPJL and DPAJL. Its day-to-day powers are delegated to the Information Commissioner, with the exception of the issuing of public statements and imposing fines.

The Authority has wide powers to require information and to enter and search premises (Schedule 1 DPAJL). It may also conduct and/or require an audit of a controller or processor.

The Information Commissioner may take the following enforcement actions:

Reprimand

The DPAJL does not specify the conditions upon which a reprimand may be issued; however most will likely take the form of a notice, and may be issued in combination with an administrative fine or a formal undertaking by the controller or processor to meet future compliance with any part of the DPJL or DPAJL.

Warning

This sanction applies where it appears to the Information Commissioner that the intended processing or other act or omission is likely to contravene the DPJL or DPAJL. Such warnings may be issued by way of a formal notice in advance of any intended processing.

Order

This refers to a formal notice of enforcement and can order any or all of the following:

- Bring specified processing operations into compliance with the DPAJL or DPJL, or take any other specified action required to comply with the same, in a manner and within a period specified in the order
- Notify a data subject of a personal data breach
- Comply with a request made by the data subject to exercise a data subject right
- Rectify or erase personal data
- Restrict or limit the recipient’s processing operations, and
- Notify persons to whom the personal data has been disclosed of the rectification, erasure or temporary restriction on processing

Administrative Fines

The DPAJL also empowers the Authority to impose administrative fines (Article 26 DPAJL), which may be imposed in addition to any other sanctions.

An administrative fine must not exceed £300,000 or 10% of the person’s total global annual turnover or total gross income in the preceding financial year, whichever is the higher (Article 27(2) DPAJL).

An administrative fine ordered against any person whose processing of data that gave rise to the fine was in the public interest and not for profit must not exceed £10,000 (Article 27(3) DPAJL).

Subject to the above limits, an administrative fine of up to £5 million may be ordered for:

- Failure to make reasonable efforts to verify that a person giving consent to the processing of the personal data of a child as required by Article 11(4) of the DPJL (information society services) is a person duly authorized to give consent to that processing
- Breach of Article 7 of the DPJL (obligations of joint controllers)
- Breach of Part 3 of the DPJL (which includes record-keeping obligations, data protection by design and default, data protection impact assessments, appointment conditions for data processors and breach notification)
- Breach of Part 4 of the DPJL (which includes information security obligations and general obligations on processors), and
- Breach of Part 5 of the DPJL (which includes obligations relating to data protection officers)

An administrative fine of up to £10 million may be imposed for:

- Breach of Part 2 of the DPJL (which includes fundamental duties of controllers, including compliance with the data protection principles, data subject information provisions and rules regarding consent) other than for Articles 7 and 11 (4), and
- Breach of Part 6 of the DPJL (Data Subject Rights)

Right to claim compensation

The DPJL makes specific provision for individuals to bring private claims against controllers and processors.

Where a controller has breached the transparency and data subject rights provisions of the DPJL, a data subject may ask the Royal Court to make such order as it considers appropriate, which may include:

- An award of compensation for loss, damage or distress in respect of the violation

- An injunction (including an interim injunction) to restrain any actual or anticipated violation
- A declaration that the controller is responsible for the violation or that a particular act, omission or course of conduct on the part of the controller would result in a violation, and
- Requiring the controller to give effect to the transparency and data subject rights provisions (unless, in the case of a data subject access request, the Royal Court is satisfied that complying with the request will cause serious harm to a third party's physical or mental health)

Any person who has suffered "loss, damage or distress" as a result of a breach of the DPJL has the right to receive compensation (Article 69 DPJL) from the controller or processor. This means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss. In addition, data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 70). Individuals also enjoy the right to lodge a complaint with the Information Commissioner in relation to any violation of the DPJL that affects him or her (Article 19 DPAJL). Last, all natural and legal persons, including individuals, controllers and processors, have the right to complain to the Royal Court about a decision, or failure to make a decision, of the Authority or Information Commissioner concerning him or her.

Offenses

The DPJL contains the following offenses:

- Unlawfully obtaining personal data (Article 71 DPJL)
- Requiring a person to produce certain records (Article 72 DPJL)
- Providing false information (Article 73 DPJL), and
- Obstruction (Article 74 DPJL)

The DPAJL contains the following offenses:

- Failing to register with the Authority as a controller or processors (Art.17(6) DPAJL), and
- Failing to comply with an order made by the Authority following a breach determination (Article 25(8) DPAJL)

If a company or other organization commits a criminal offense under the DPJL or DPAJL, any partner, director, manager, secretary or similar officer or someone purporting to act in such capacity is personally guilty of an offense in addition to the corporate body if:

- The offense was committed with his or her consent or connivance, or
- The offense is attributable to any neglect on his or her part

ELECTRONIC MARKETING

The DPJL applies to most electronic marketing activities, as they involve some use of personal data (e.g. an email address that includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller.

Where consent is relied upon, the strict standards for consent under the DPJL apply, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the checking of an unchecked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 36 DPJL).

ONLINE PRIVACY

Jersey has no specific law regulating online privacy; however, the DPJL and DPAJL generally apply.

KEY CONTACTS

Carey Olsen Jersey LLP
www.careyolsen.com

Huw Thomas
Partner
Carey Olsen Jersey LLP
T +44 1534 888900
huw.thomas@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

JORDAN

Last modified 11 January 2024

LAW

Personal data protection is regulated in Jordan under the Law of Personal Data Protection No. (24) of the Year 2023 (the “Law”). Jordan took a serious steps to enact this legislation aimed at the protection of personal data. The Data Protection law was published in the Official Gazette no. 5881 page 4338 on 17 September 2023.

Details on the law

Within this Law, numerous restrictions are placed on the processing of personal data, the most important and notable one being the requirement for prior consent being “explicit and documented in writing or electronically, it should also be specific in terms of duration and purpose.” The Law also stipulates that citizens should be informed in advance of their data’s date and reasons for collection. It also criminalizes the processing of data for reasons other than the purpose intended.

As for now, all communications that may contain personal information are protected and private under Article 18 of the Jordanian Constitution, which states that “All postal and telegraphic correspondence, telephonic communications, and other communications means shall be regarded as secret and shall not be subject to censorship, viewing, suspension or confiscation except by a judicial order in accordance with the provisions of the law”. Additionally, Article (7) states that personal freedom shall be protected, and that any infringement of the rights and public freedoms or sanctity of private life of Jordanians is a crime punishable by law.

Personal information protection in the public sector is regulated in Jordan under a specific law. Article 18 of the Jordanian Constitution in addition to the Data Protection law are applicable to both private and public sector.

The right of privacy is protected under the Jordanian Constitution and Law of Personal Data Protection. In accordance with the Data Protection Law, a public authority may process personal data without prior consent or notifying the person if the processing is carried out directly by a competent public authority to the extent required to carry out the tasks entrusted to it by law or through other contracted parties, provided that the contract (in case a governmental entity assigns its duties to another party to provide it services by signing a contract, then this contract must adhere to the provisions of the Data Protection Law). This includes observance of all obligations and conditions stipulated in this law and the regulations and instructions issued pursuant thereto.

Article (6) of the same provides for exceptions to the requirement of prior consent, as follows:

1. Processing carried out directly by a competent Public entity to the extent required to carry out the tasks entrusted to it in accordance with the provisions of the legislation in force or through other contracting parties provided that the contract includes compliance with all obligations and conditions stipulated in this Law and the regulations and instructions issued pursuant thereto.
2. If necessary to preventine medical purpose medical diagnosis or provision of health care by a licensee licensed to practice any of the medical professions.

3. If necessary to protect the life of the concerned person or his vital interests.
4. If necessary for the prevention of a crime or for its detection by a competent authority for the prosecution of crimes committed in violation of the provisions of the Law.
5. If required or authorized by virtue of any legislation or in implementation thereof or by virtue of a decision of the competent court.
6. If required for the purposes of the entities subject to the control and supervision of the Central Bank of Jordan to carry out their activities as determined by the Central Bank of Jordan including the transfer and exchange of data inside or outside the Kingdom.
7. The treatment carried out in accordance with the provisions of the Regulations issued pursuant to the provisions of this Law.
8. If necessary for the purposes of scientific or historical research if they are not intended to take any decision or action with respect to a specific person.
9. If necessary for statistical purposes or national security requirements or achieve the public interest.
10. If the subject of the processing is publicly available data from the Person concerned.

Article (15) of the law, relating to the cross-border transfer of personal data outside of the Hashemite Kingdom of Jordan, states that:

1. Regional or international judicial cooperation under international conventions or treaties in force in the Kingdom.
2. Regional or international cooperation between the Kingdom and international or regional bodies, organizations or agencies working in the field of combating crime of all kinds or prosecuting the perpetrators.
3. Exchange of personal medical data of the person concerned with processing when necessary for processing and exchange of data related to epidemics or health disasters or what affects public health in the Kingdom.
4. Exchange of data related to epidemics or health disasters or what affects public health in the Kingdom.
5. Transfer my occur if the concerned individual provides explicit consent after being informed that an adequate level of protection is unavailable.
6. Transactions involving banking operations and money transfers outside the Kingdom.

Before initiating the Data transfer, the Official is obligated to verify the level of protection guaranteed by the Recipient outside the Kingdom, ensuring the safety and security of the Data.

Article (7) of the Law, carries on specifying the Special conditions for the processing (which includes transferring or sharing) of personal datalt is prohibited to process personal data without the consent (standard of consent is set out above).

It is impermissible to conduct processing of personal data for anyone whom is incapacitated, without the prior written or electronic consent of one of his parents, and in the absence of a parent for any reason, the consent of the legally appointed guardian is taken to follow up on his affairs.

As for the processing of sensitive personal data, the following conditions apply: As per Article (6) of the Law, It is prohibited to process sensitive personal data without the prior approval of the concerned person, except in the following cases:

1. Processing carried out directly by a competent Public entity to the extent required to carry out the tasks entrusted to it in accordance with the provisions of the legislation in force or through other contracting parties provided that the contract includes compliance with all obligations and conditions stipulated in this Law and the regulations and instructions issued pursuant thereto.
2. If necessary to preventine medical purpose medical diagnosis or provision of health care by a licensee licensed to practice any of the medical professions.
3. If necessary to protect the life of the concerned person or his vital interests.
4. If necessary for the prevention of a crime or for its detection by a competent authority for the prosecution of crimes committed in violation of the provisions of the Law.
5. If required or authorized by virtue of any legislation or in implementation thereof or by virtue of a decision of the competent court.

6. If required for the purposes of the entities subject to the control and supervision of the Central Bank of Jordan to carry out their activities as determined by the Central Bank of Jordan including the transfer and exchange of data inside or outside the Kingdom.
7. The treatment carried out in accordance with the provisions of the Regulations issued pursuant to the provisions of this Law.
8. If necessary for the purposes of scientific or historical research if they are not intended to take any decision or action with respect to a specific person.
9. If necessary for statistical purposes or national security requirements or achieve the public interest.
10. If the subject of the processing is publicly available data from the Person concerned.

The protection officer, personal data processor and recipient of personal data are committed to ensuring the integrity and security of personal data and tracking cases of abuse of personal data security. The personal data must be handled and processed in such a way that ensures confidentiality, safety, and non-modification.

DEFINITIONS

Definition of Personal Data

There is no specific definition in the laws or the regulations.

Definition of Sensitive Personal Data

There is no specific definition in the laws or the regulations.

NATIONAL DATA PROTECTION AUTHORITY

Not applicable.

REGISTRATION

No registration required.

DATA PROTECTION OFFICERS

Not applicable at present, but see details on the draft law.

COLLECTION & PROCESSING

The legislations in Jordan are silent in this regard, however see details on the draft law.

TRANSFER

The Cybercrime Law No. (27) of 2015 (‘**Cybercrime Law**’) generally acts to criminalise unlawful access to websites or information systems such as access without authorisation, permission or in a manner that breaches the said authorisation or permission.

Anyone who intentionally enters a computer network or an information system by any means without authorisation, or in violation of or exceeding the authorisation, shall be punished by imprisonment for a period of no less than a week and not exceeding three months, or by a fine of no less than (100) one hundred dinars and not more than (200) two hundred dinars, or both of these penalties.

If the entry stipulated above is accompanied with the intention to cancel, delete, add, destroy, disclose, damage, withhold, modify, change, transfer or copy data or information, or stop or disrupt the work of the information network or the information network information system, then the offender shall be imprisoned for a period of not less than three months and not exceeding one year and a fine of no less than (200) two hundred dinars and not more than (1,000) one thousand dinars.

SECURITY

Anyone who intentionally enters the information network or information system by any means without permission, or in violation of or exceeding authorisation with the aim of accessing data or information not available to the public and that affects national security, foreign relations of the Kingdom, public safety or the national economy shall be punished with imprisonment for a period of no less than four months and a fine of no less than (500) five hundred dinars and not more than (5000) five thousand dinars.

If the entry referred to above is accompanied with the intention of cancelling, destroying, modifying, changing, transferring, copying or disclosing such data or information, the perpetrator shall be punished with temporary labour and a fine of no less than (1,000) thousand dinars and not more than (5000) five thousand dinars.

Anyone who intentionally accesses a website to view data on information not available to the public that affects national security, the Kingdom’s foreign relations, public safety, or the national economy shall be punished by imprisonment for a period of no less than four months and a fine of no less than (500) five hundred dinars.

If the entry referred to in the paragraph directly above is accompanied with the intention to cancel, destroy, modify, change, move or copy such data or information, the perpetrator shall be punished with temporary labour and a fine of no less than (1,000) one thousand dinars and not more than (5,000) five Thousands of dinars.

BREACH NOTIFICATION

In the relation to the Cybercrimes, the injured party shall have the right to submit a complaint before the Cybercrime Unit and the latter shall review the complaint and transfer it to the court.

Mandatory breach notification

It is stated in the aforementioned draft Personal Data Protection law, under Article (6), that a unit will be established within the Ministry of Digital Economy and Entrepreneurship, which will be responsible for preparing a regulation that controls the process of receiving notifications and complaints regarding any violations that may affect personal data.

The second law is “Cyber Security Law No. 16 of 2019” as it has established a National Center for Cyber Security, which receives complaints and reports related to cyber security and cyber security incidents. The law opened the door for further collaboration with different official entities according to its sphere of specialty.

The Cybersecurity Framework for Jordan Financial Sector – V. 1 – July, 2021, states that organizational-level severity rating is performed by the entity to define the point at which the incident should be treated as a disaster, in addition to determine escalation procedures, as well as human resources and time durations to recover. The entity has to notify the Central Bank of Jordan / Financial Cyber Emergency Response Team about the incident according to the following timelines:

- Initial notification within 2 hours from confirming time.
- After the closure of the incident for “Low” incidents.
- Within 8 hours from confirming the incident and one time every two business days for “Medium” incidents.
- Within 4 hours from confirming the incident and once a day for “High” incidents.

Additionally, Article (49) of the Instructions for Handling Cyber Risks No. (26/1/1/1984) for the Year 2018 stipulates that *“ the company shall notify the Central Bank in the event of discovering that it has been exposed to any cyber incident or any attempt of cyber-attack characterised by a high degree of danger to its systems or networks, no later than 72 hours from the moment of discovery of the cyber-event and according to the mechanism that will be adopted by the Central Bank, and inform the relevant security services of any case of embezzlement, forgery, theft or fraud resulting from the cyber event as soon as it is discovered and in accordance with the relevant laws and instructions.”*

ENFORCEMENT

The Cybercrime Unit is the body responsible to deal with any complaints and to assign it to the court.

In general, the court shall enforce the sanctions that are stated in the Cybercrime Law, and any other applicable laws and regulations.

ELECTRONIC MARKETING

The e-Procurement Instructions of 2018 mandates the use of JONEPS (Jordan Online E-Procurement System) in the implementation of public procurement.

The user of the system means the government entity, government unit, or interested party that submitted an application for registration on the electronic system and was approved by the electronic system manager.

The instructions explicitly state that the user of the system shall maintain the confidentiality of the information available in the system and take all necessary precautions and measures that would prevent the leakage of any information to any person, including the following:

- Prevent the disclosure of information to persons who are not authorised to view or disclose it, and apply the highest levels of privacy, confidentiality, security and transparency of information.
- Maintaining the security and integrity of data from alteration or modification by any party that does not have the authority to do so.

Additionally, the tenderer shall provide security controls to protect the system and devices, such as using anti-virus programs, using strong and modern programs and programs to detect intrusions from people or programs, and constantly updating information security programs.

Finally, the user of the system must use the system in a safe and sound manner, and it bears responsibility for any wrong use by it or by its users.

ONLINE PRIVACY

The legislations in Jordan are silent in this regard.

KEY CONTACTS

Aljazy& Co.
www.aljazylaw.com/

Omar M.H. Aljazy
Managing Partner
Aljazy& Co.
T + (962 6) 5654477
oaljazy@aljazylaw.com

Sewar Smierat
Head of Corporate Department
Aljazy& Co.
T + (962 6) 5654477
ssmierat@aljazylaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

KAZAKHSTAN

Last modified 11 January 2024

LAW

The main legal act regulating personal data in Kazakhstan is the law of the Republic of Kazakhstan No. 94-V dated May 21, 2013 'On Personal Data and Its Protection' (the 'Law').

There are also a number of other laws providing for personal data protection requirements, including:

- The Law on Informatisation;
- The Law on Communication;
- The Labour Code of Kazakhstan;
- The Law on Online Platforms and Online Advertising.

DEFINITIONS

Definition of personal data

'**Personal data**' is any information relating to a specific individual (personal data subject) or a personal data subject who can be identified on the basis of such information which is recorded on electronic, paper and / or another tangible medium.

The law divides personal data into:

- '**Generally accessible personal data**', which is personal data that can be accessed freely with the consent of the personal data subject or to which confidentiality requirements do not apply in accordance with Kazakh law; and
- '**Limited access personal data**', which is personal data, access to which is limited by Kazakh law

Definition of sensitive personal data

Kazakh law does not provide for express definition of sensitive personal data.

In certain cases, sensitive personal data may qualify as limited access personal data and, as such, it is additionally regulated by sector-specific laws of Kazakhstan (e.g. medical secrecy, subscriber data). In our replies, we do not consider sector-specific restrictions which may affect personal data regulation (e.g. Kazakh law prohibits transfer of subscriber data, which includes, *inter alia*, personal data of subscribers).

NATIONAL DATA PROTECTION AUTHORITY

The main state authority in the field of personal data protection is the Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan (the ‘Ministry’). The Ministry:

- shapes and implements the state policy on personal data and its protection;

- develops the procedure for implementation of personal data protection measures by the owner and / or operator of a personal data database and a third party related to the owner and / or operator of a personal data database;
- develops the rules to be followed by the personal data database owner and (or) operator when determining the scope of personal data necessary and sufficient for the performance of their tasks;
- develops the procedure for determining the list of personal data necessary and sufficient for the performance of tasks by the owner and (or) operator of a personal data database;
- determines the procedure for implementation of personal data protection measures by the owner and (or) operator of a personal data database, as well as by a third party;
- reviews requests of a personal data subject or his / her legal representative on compliance of the content of personal data and methods of its processing with the purpose of its processing and makes a respective decision;
- takes measures on bringing persons who have violated personal data laws of Kazakhstan to liability in accordance with the laws of Kazakhstan;
- requests the owner and / or operator of a personal data database and a third party related to the owner and / or operator of a personal data database to clarify, block or destroy inaccurate or illegally obtained personal data;
- takes measures on improving protection of rights of personal data subjects;
- creates an advisory council on issues of personal data and its protection as well as determines the procedure for its formation and activities;
- approves the rules for collection and processing of personal data;
- approves the rules for conducting a survey in order to assess the security level when storing, processing and distributing limited access personal data contained in electronic information resources and such rules should be agreed with the National Security Committee of the Republic of Kazakhstan;
- approves the rules for the functioning of the state service for control of access to personal data;
- coordinates the integration of non-state informatization entities with the state informatization entities and (or) state legal entities, which involves personal data transfer and (or) provision of access to personal data;
- approves the rules for integration with the state service for control of access to personal data;
- exercises other powers provided by Kazakh law.

The Government of Kazakhstan develops the main directions of state policy on personal data and its protection.

In relation to personal data and its protection, state authorities (each within its competence):

- develop and / or approve regulatory acts;
- consider appeals of individuals and / or legal entities regarding personal data and protection of personal data issues;
- take measures for bringing persons who have violated personal data legislation of Kazakhstan to liability;
- exercise other powers provided for by Kazakh law.

Supervision over observance of Kazakh law in respect of personal data and its protection is carried out by the prosecution authorities of Kazakhstan.

REGISTRATION

Under Kazakh law, there is no express registration requirement in relation to personal data and its protection, except the requirement for the personal data database owner and (or) operator as well as a third party related to the owner and / or operator to register and keep a record of the following actions:

- the term or period during which the consent to the collection, processing of personal data is valid;
- information on whether there is a possibility of transfer of personal data to third parties by the personal data operator or not;
- information on whether there is a cross-border transfer of personal data as part of the personal data processing;
- information on dissemination of personal data in publicly resources.

DATA PROTECTION OFFICERS

Under Kazakh law, an owner and / or operator of a personal data database, which is a legal entity, should appoint a person responsible for organizing the processing of personal data. Such person is obliged to:

- exercise internal control over observance by the owner and / or operator of a personal data database and its employees of Kazakh law requirements in relation to personal data and its protection;
- inform the employees of an owner and / or operator of the provisions of Kazakh law in respect of processing and protection of personal data;
- exercise control over receipt and processing of applications from personal data subjects or their legal representatives.

In addition, an owner and / or operator of a database containing personal data and a third party related to the owner and / or operator should, *inter alia*, when collecting and processing personal data, determine list of persons carrying out collection and processing of personal data or having access to it.

COLLECTION & PROCESSING

Kazakh law requires to carry out collection and processing of personal data with the consent of a personal data subject or his / her legal representative. Such consent should be given in writing, via the state service, non-state service or other method that allows to confirm the receipt of consent. The consent should be given via the state service when collecting and / or processing personal data contained in the databases of the state bodies and / or state legal entities.

As a general rule, personal data subjects or their representatives may revoke their consent. However, the consent may not be revoked in cases where such revocation contradicts requirements of Kazakh law or there are any unfulfilled obligations.

Consent to the collection and processing of personal data should include:

- full name, business identification number (individual identification number) of the personal data database operator;
- full name of the personal data subject;
- the term and period during which the consent is effective;
- information on whether the operator may transfer the personal data to third parties or not;
- information on whether there is a cross-border transfer of personal date in the process of its processing or not;
- information on dissemination of personal data in public resources;
- list of data being collected on the personal data subject;
- other information as determined by the owner and / or operator.

Kazakh law allows the collection and processing of personal data without the consent of a personal data subject or his / her legal representative in cases explicitly prescribed by Kazakh law. Such cases may include, inter alia:

- implementation of activities of law enforcement bodies and courts;
- implementation of state statistical activities;
- use of depersonalised personal data by the state authorities for statistical purposes;
- implementation of international treaties ratified by Kazakhstan;
- protection of constitutional rights and freedoms of a person, if obtaining the consent of a personal data subject or his / her legal representative is impossible;
- carrying out legal professional activities of a journalist, carrying out tv-channel, radio-channel, news agency, mass media, online media, scientific, literary or other creative activities, subject to compliance with requirements of Kazakh law;
- publication of personal data in accordance with Kazakh law, including personal data of candidates for elective public offices;
- failure by a personal data subject to fulfil its obligation to provide personal data in accordance with Kazakh law;
- receipt by the state authority regulating, controlling and supervising financial market and financial organisations of information from individuals and legal entities in accordance with Kazakh law;
- receipt by the state revenue authorities of information from individuals and legal entities for purposes of tax administering and control;
- storage of a backup copy of electronic information resources containing limited access personal data to a national backupplatform for storing electronic information resources in cases provided for by Kazakh law;

- the use of personal data of entrepreneurs related directly to their business activities to form a register of business partners, subject to compliance with the requirements of Kazakh law;
- the use of personal data of a Kazakhstani national for the purposes of bankruptcy procedure.

Under the Law, processing of personal data should be limited to the achievement of specific, predetermined and legitimate goals. Processing of personal data that is incompatible with the purposes of collecting personal data is not allowed. Personal data, the content and volume of which is excessive in relation to the purposes of its processing, should not be processed.

Under Kazakh law, access to personal data is determined by the terms of consent for collection and processing of personal data, unless otherwise provided by Kazakh law. A person should be denied access to personal data if he / she refuses to assume obligations to ensure compliance with the requirements of the Law or may not ensure it.

Persons having access to limited access personal data should ensure its confidentiality.

Under Kazakh law, accumulation of personal data is carried out by collecting personal data that is necessary and sufficient to fulfil the tasks performed by an owner and / or an operator of a database containing personal data and by a third-party having access to such database.

Personal data should be stored in databases located in Kazakhstan.

The period for retention of personal data is determined by the date of fulfilment of the purpose(s) for collection and processing of the personal data, unless otherwise provided by Kazakh law.

Kazakh law provides for additional requirements in respect of electronic resources containing personal data and integration between personal data databases of private entities and the personal data databases of state bodies and state legal entities via the state service.

TRANSFER

Transfers of personal data are allowed if they do not violate the rights and freedoms of a personal data subject and do not affect the legitimate interests of other individuals and / or legal entities.

The transfer of personal data in cases that go beyond the previously stated purposes of its collection is permitted if carried out with the consent of a personal data subject or his / her legal representative.

The cross-border transfer of personal data to other countries is carried out only in cases where such countries ensure protection of personal data.

The cross-border transfer of personal data to countries that do not ensure protection of personal data is possible:

- with the consent of the personal data subject or his / her legal representative to the cross-border transfer of his / her personal data;
- in cases stipulated by international treaties ratified by Kazakhstan;
- in cases provided for by Kazakh law, if it is necessary for protecting the constitutional system, public order and public health and morals and rights and the freedoms of a person in Kazakhstan;
- in case of protection of constitutional rights and freedoms of a person, if obtaining the consent of a personal data subject or his / her legal representative is impossible.

Kazakh law may in certain cases prohibit the cross-border transfer of personal data.

SECURITY

Protection of personal data is guaranteed by the state and is carried out in a manner determined by the Ministry.

Collection and processing of personal data is carried out only if its protection is ensured. Kazakh law defines protection of personal data as a set of legal, organization and technical measures.

The owner and / or operator of a personal data database and a third party having access to such database are required to take measures for protecting personal data in a manner determined by the Ministry, which ensure:

- prevention of unauthorized access to personal data;
- timely detection of the facts relating to an incident of unauthorized access to personal data, if
- such unauthorized access could not be prevented;
- minimizing adverse effects of unauthorized access to personal data;
- the state technical service’s access to objects of informatisation that use, store, process and distribute limited access personal data contained in electronic information resources, so that the state technical service could carry out a survey to assess the security level of the processes of storage, processing and distribution of limited access personal data contained in electronic information resources in the manner determined by the authorized body;
- registration of certain operations with the personal data where required by Kazakh law.

The obligations of an owner and / or operator of a database containing personal data and a third party having access to such database to protect personal data arise from the moment of collecting the personal data and remain in force until such personal data is destroyed or depersonalized.

Kazakh law provides for additional requirements with regard to protection of electronic resources containing personal data.

BREACH NOTIFICATION

An owner and / or operator of a database containing personal data should notify the authorized state body of security incidents related to an illegal access to the personal data of limited access.

ENFORCEMENT

Generally, all state authorities of Kazakhstan, depending on their competences, may consider appeals of individuals and / or legal entities regarding personal data and protection of personal data issues. The Ministry is authorised to take measures against persons who have violated the personal data legislation of Kazakhstan.

Prosecution Authorities of Kazakhstan carry out supervision over compliance with personal data legislation of Kazakhstan and may also take measures on bringing persons who have violated personal data legislation of Kazakhstan to liability. Interested persons may file complaints to the Prosecutor’s Office and the Ministry regarding breach of the legislation in relation to personal data and its protection.

Kazakh law provides for administrative and criminal liability for violation of Kazakh law in relation to personal data and its protection.

ELECTRONIC MARKETING

The Law on Online Platforms and Online Advertising provides for certain requirements for personal data protection in relation to the use of online platforms (websites, messengers, etc.) and online advertising.

In particular, it prohibits the profiling of the online-platform’s users for the purposes of targeted advertising if such profiling is based on race or nationality, political opinions, biometric or personal data, or information about the users’ health. Profiling is defined as a set of algorithms aimed at determining the preferences and (or) interests of users.

ONLINE PRIVACY

Under the Law on Online Platforms and Online Advertising, the owner and (or) legal representative of the relevant online platform should do the following in order to protect personal data on the online platform:

- familiarize users with the privacy policy of the online platform before completing their registration;
- ensure the integrity, safety and confidentiality of personal data;
- prevent the dissemination of personal data without the consent of the user or his / her legal representative;
- immediately notify the user in case of violation of the confidentiality of his / her personal data;

- perform other duties provided for by the Law on Personal Data and Its Protection.

KEY CONTACTS

Dinara Jarmukhanova
Partner, Head of Kazakh practice
Centil Law Firm
T +7 727 315 0784
dinara.jarmukhanova@centil.law

Dariga Adanbekova
Associate
Centil Law Firm
T +7 727 315 0784
dariga.adanbekova@centil.law

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

KENYA

Last modified 12 January 2023

LAW

The Data Protection Act, 2019 (the “**Act**”) came into force on 25th November, 2019 and is now the primary statute on data protection in Kenya. It gives effect to Article 31 c) and d) of the Constitution of Kenya, 2010 (right to privacy).

In October 2020, by virtue of the powers conferred to him under the Act, the Cabinet Secretary for Information, Communication, Technology, Innovation and Youth Affairs gazetted the Data Protection (Civil Registration) Regulations, 2020 (the “**Regulations**”). The Regulations apply to civil registries involved in processing personal data for registrations such as births, deaths, adoptions, persons, passports and marriages.

Since the Data Protection Commissioner’s (DPC) appointment on 16 November 2020, significant efforts have been made in developing regulations for the implementation of the Act.

- **Data Protection (Compliance & Enforcement) Regulation, 2021** – sets out the complaints handling procedures and enforcement mechanisms in the event of non-compliance with the provisions of the Act;

- **Data Protection (Registration of Data Controllers & Data Processors) Regulations, 2021** – provides for the registration of data controllers and data processors with the DPC. The threshold for mandatory registration is also set out under these regulations; and

- **Data Protection (General) Regulations, 2021** – elaborates in more detail the rights of data subjects, restrictions on commercial use of personal data, duties and obligations of data controllers and data processors, elements of implementing data protection by design or default, notification of personal data breaches, transfer of personal data outside Kenya, conduct of data protection impact assessment and other general provisions.

The above regulations were gazetted in January and came into effect on 14 February 2022 with the exception of the Data Protection (Registration of Data Controllers & Data Processors) Regulations, 2021 which came into force on 14 July 2022.

The DPC has also issued a number of guidelines, these include:

- **Guidance Note on Registration of Data Controllers and Data Processors** - developed to assist entities in ascertaining if they are data controllers or data processors, and to understand their obligations with respect to mandatory registration;
- **Guidance Note on Processing Personal Data for Electoral Purposes** - developed to assist data controllers and data processors dealing with voters’ personal data and members of political parties’ personal data to understand their obligations under the Act;
- **Guidance Note on Data Protection Impact Assessment** - to assist data controllers and data processors to understand their obligations under the Act and the need to undertake a Data Protection Impact Assessment; and

- **Guidance Note on Consent** - developed to assist data controllers and data processors to understand their duties under the Act and their obligations as far as obtaining consent is concerned.

The DPC has also published a **Complaints Management Manual** which sets out the complaints management handling procedure by the DPC; and the **Alternative Disputes Resolution Framework** which provides guidance to stakeholders who wish to engage in Alternative Dispute Resolution (ADR) to resolve their disputes arising under the Act.

DEFINITIONS

Definition of personal data

Section 2 of the Act

Personal data is defined as data relating to an identified or identifiable natural person.

Definition of sensitive personal data

Section 2 of the Act

Sensitive personal data is defined as data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.

NATIONAL DATA PROTECTION AUTHORITY

Part II of the Act

The Act established the Office of the Data Protection Commissioner (DPC) whose mandate includes overseeing the implementation and enforcement of the provisions of the Act. The DPC is also tasked with the maintenance of the register of data controllers and processors, receiving and investigation of complaints under the Act and carrying out inspections of public and private entities to evaluate the processing of personal data.

REGISTRATION

Section 18 of the Act

Data processors and data controllers are required to be registered with the DPC. The DPC, however, has discretion to prescribe the thresholds for mandatory registration based on:

- the nature of industry;
- the volumes of data processed; and
- whether sensitive personal data is being processed.

The Data Protection (Registration of Data Controllers & Data Processors) Regulations, 2021, provides for the registration of data controllers and data processors with the DPC. The threshold for mandatory registration is also set out under these regulations. The DPC also launched a portal where applications for registration are submitted in the prescribed form and upon payment of a prescribed fee. Where the DPC is satisfied that the applicant has fulfilled the requirements for registration, a certificate of registration is issued within 14 days and entry of the applicant’s details is made in the register of data controllers and data processors.

The certificate of registration issued is valid for 24 months from the date of issuance.

A data controller or data processor with an annual turnover or revenue of below Kenya Shillings Five Million (approx. USD 40,000) and has less than 10 employees is exempt from mandatory registration.

Data controllers and data processors who process data for the following purposes regardless of their annual turnover or revenue or number of employees have to be registered under the Regulations:

- canvassing political support among the electorate;
- crime prevention and prosecution of offenders (including operating security CCTV systems);
- gambling;
- operating an educational institution;
- health administration and provision of patient care;
- hospitality industry firms, excluding tour guides;
- property management including the selling of land;
- provision of financial services;
- telecommunications network or service providers;
- businesses that are wholly or mainly in direct marketing; and
- transport services firms (including online passenger hailing applications); and businesses that process genetic data.

DATA PROTECTION OFFICERS

Section 24 of the Act

The Act makes provisions for the designation of Data Protection Officers (DPOs) but this obligation is not mandatory.

DPOs can be members of staff and may perform other roles in addition to their roles. A group of entities can share a DPO and the contact details of the DPO must be published on the organisation’s website and communicated to the DPC.

DPOs have the following roles:

- advising the data controller or data processor and their employees on data processing requirements provided under the Act or any other written law;
- ensuring compliance with the Act;
- facilitating capacity building of staff involved in data processing operations;
- providing advice on data protection impact assessment; and
- co-operating with the DPC and any other authority on matters relating to data protection.

DPO’s under the Regulations also have the following additional roles:

- monitoring and evaluating the efficiency of the data systems in the organization; and
- keeping written records of the processing activities of the civil registration entity.

COLLECTION & PROCESSING

Section 25 of the Act

The processing of personal data must comply with the principles prescribed in this part. It must be:

- processed in accordance with the right to privacy of the data subject;
- processed lawfully, fairly and in a transparent manner in relation to any data subject;
- collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;
- collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
- accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
- kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and
- not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

Section 30 of the Act

The Act recommends personal data to be collected and processed lawfully. The lawful reasons for processing include:

a. Consent of the data subject; or
b. the processing is necessary:
    - for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
    - for compliance with any legal obligation to which the controller is subject;
    - in order to protect the vital interests of the data subject or another natural person;
    - for the performance of a task carried out in the public interest or in the exercise of
        - official authority vested in the controller;
        - the performance of any task carried out by a public authority;
    - for the exercise, by any person in the public interest, of any other functions of a public nature;
    - for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or
    - for the purpose of historical, statistical, journalistic, literature and art or scientific research.

It is an offence to process personal data without a lawful reason.

Under the Regulations civil registration entities must ensure that they collect only personal data permitted by the data subject and that the appropriate steps are taken to ensure the quality and security of the personal data.

Where the registries intend to use such data for another purpose, they must either ensure that the purpose is compatible with the initial purpose or, where that is not the case, seek fresh consent.

The Data Protection (General) Regulations, 2021 elaborate in more detail restrictions on commercial use of personal data, duties and obligations of data controllers and data processors, elements of implementing data protection by design or default, conduct of data protection impact assessment and other general provisions.

TRANSFER

Part VI of the Act

The transfer of personal data outside Kenya is highly regulated under the Act. Prior to any transfer the data controller or data processor must provide proof to the DPC on the appropriate safeguards with respect to the security and protection of the personal data including jurisdictions with similar data protection laws.

The consent of the data subject is required for the transfer of sensitive personal data out of Kenya.

Under the Regulations, civil registration registries cannot transfer personal data collected for civil registration purposes outside Kenya without the written approval of the DPC.

The Data Protection (General) Regulations, 2021 elaborate in more detail transfer of personal data outside Kenya. The Regulations provide for 4 legal bases for the transfer of personal data out of the country which include;

a. appropriate data protection safeguards in the country or territory where recipient is based in;
b. adequacy: an adequacy decision made by the DPC that the country, territory or the international organization where data is being transferred ensures an adequate level of protection of personal data;
c. necessity: transfer is deemed to be necessary if it is:
    - for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
    - for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;
    - for any matter of public interest;

- for the establishment, exercise or defence of a legal claim in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

d. consent of the data subject on the condition they have consented to the proposed transfer and have been informed of the possible risks of transfer.

SECURITY

Sections 41 and 42 of the Act

Data controllers and processors are required to implement the appropriate organizational and technical measures to implement data protection principles in an effective manner.

Civil registration registries are mandated to formulate written data security procedures which must include the following:

- instructions concerning physical protection of the database sites and their surroundings;
- access authorizations to the database and database systems;
- description of the means intended to protect the database systems and the manner of their operation for this purpose;
- instructions to authorized officer of the database and database systems regarding the protection of data stored in the database;
- the risks to which the data in the database is exposed in the course of the civil registration entity's ongoing activities;
- the manner of dealing with information security incidents, according to the severity of the incident;
- instructions concerning the management and usage of portable devices;
- instructions with respect to conducting periodical audits to ensure that appropriate security measures, in accordance with the Procedure and these Regulations exist; and
- instructions regarding backup of personal data.

As far as technical measures are concerned, the Regulations require the use of hashing and cryptography to limit the possibility of repurposing personal data. The Regulations also require that the contract between a data controller and a data processor to include a clause on security measures subjecting the data processor to appropriate technical and organizational measures in relation to keeping personal data secure.

With respect to organizational measures, the Regulations require a data controller or data processor to develop, publish and regularly update a policy reflecting their personal data handling practices. The policy may include:

a. the nature of personal data collected and held;
b. how a data subject may access their personal data and exercise their rights in respect to that personal data;
c. complaints handling mechanisms;
d. lawful purpose for processing personal data;
e. obligations or requirements where personal data is to be transferred outside the country, to third parties, or other data controllers or data processors located outside Kenya and where possible, specify such recipients;
f. the retention period and schedule; and
g. the collection of personal data from children, and the criteria to be applied.

The Regulations provide for specific obligations to the data controller and data processor under the data protection principle of integrity, confidentiality and availability. These include:

a. having an operative means of managing policies and procedures for information security;
b. assessing the risks against the security of personal data and putting in place measures to counter identified risks;
c. processing that is robust to withstand changes, regulatory demands, incidents, and cyber-attacks;
d. ensuring only authorised personnel have access to the data necessary for their processing tasks;
e. securing transfers shall be secured against unauthorised access and changes;

f. securing data storage from use, unauthorised access and alterations;
g. keeping back-ups and logs to the extent necessary for information security;
h. using audit trails and event monitoring as a routine security control;
i. protecting sensitive personal data with adequate measures and, where possible, kept separate from the rest of the personal data;
j. having in place routines and procedures to detect, handle, report, and learn from data breaches; and
k. regularly reviewing and testing software to uncover vulnerabilities of the systems supporting the processing.

BREACH NOTIFICATION

Breach Notification

Section 43 of the Act

As far as technical measures are concerned, the Regulations require the use of hashing and cryptography to limit the possibility of repurposing personal data. The Regulations also require that the contract between a data controller and a data processor to include a clause on security measures subjecting the data processor to appropriate technical and organizational measures in relation to keeping personal data secure.

With respect to organizational measures, the Regulations require a data controller or data processor to develop, publish and regularly update a policy reflecting their personal data handling practices. The policy may include:

a. the nature of personal data collected and held;
b. how a data subject may access their personal data and exercise their rights in respect to that personal data;
c. complaints handling mechanisms;
d. lawful purpose for processing personal data;
e. obligations or requirements where personal data is to be transferred outside the country, to third parties, or other data controllers or data processors located outside Kenya and where possible, specify such recipients;
f. the retention period and schedule; and
g. the collection of personal data from children, and the criteria to be applied.

The Regulations provide for specific obligations to the data controller and data processor under the data protection principle of integrity, confidentiality and availability. These include:

a. having an operative means of managing policies and procedures for information security;
b. assessing the risks against the security of personal data and putting in place measures to counter identified risks;
c. processing that is robust to withstand changes, regulatory demands, incidents, and cyber-attacks;
d. ensuring only authorised personnel have access to the data necessary for their processing tasks;
e. securing transfers shall be secured against unauthorised access and changes;
f. securing data storage from use, unauthorised access and alterations;
g. keeping back-ups and logs to the extent necessary for information security;
h. using audit trails and event monitoring as a routine security control;
i. protecting sensitive personal data with adequate measures and, where possible, kept separate from the rest of the personal data;
j. having in place routines and procedures to detect, handle, report, and learn from data breaches; and
k. regularly reviewing and testing software to uncover vulnerabilities of the systems supporting the processing.

Mandatory Breach Notification

Yes. Please see above analysis under “Breach Notification”.

ENFORCEMENT

The DPC has the duty to ensure the implementation and enforcement of the Act.

The Data Protection (Compliance & Enforcement) Regulation, 2021 sets out the complaints handling procedures and enforcement mechanisms in the event of non-compliance with the provisions of the Act. The Regulations provide for the process and procedure of lodging of complaints with the DPC.

The DPC is also required to maintain an up-to-date register of complaints stating the particulars of the complainant and complaint.

Section 62 of the Act

In instances where the DPC is satisfied that any person has violated the provisions of the Act, he has the power to issue penalty notices for up to a maximum of Kenya Shillings Five Million (approximately USD 50,000) or 1% of an undertaking’s annual turnover the preceding year, whichever is lower.

In addition, any act which constitutes an offence under the Act where a penalty is not provided attracts a fine of up to Kenya Shillings Three Million (approx. USD 30,000) or imprisonment for up to 10 years or both a fine and imprisonment.

Under the Data Protection (Compliance & Enforcement) Regulations, 2021 the DPC has the power to issue an enforcement notice where a person fails to comply with the provisions of the Act or the Regulations. A penalty notice is issued where there is failure to comply with the enforcement notice. The penalty notice will contain the reasons why the DPC is imposing a penalty, the administrative fine imposed, how the fine is to be paid and the rights of appeal the decision. The DPC may impose a daily fine of not more than Ksh. 10,000 (approx. USD 100/-) for each penalty identified, until the breach is rectified.

ELECTRONIC MARKETING

Section 37 of the Act

The use of personal data for commercial purposes is prohibited unless the person undertaking this processing:

- has sought and obtained express consent from a data subject; or
- is authorized to do so under any written law and the data subject has been informed of such use when collecting the data from the data subject.

The General Regulations states that a data controller or data processor is considered to be using personal data for commercial purposes if the personal data of a data subject is used to advance commercial or economic interests, including inducing another person to buy, rent, lease, join, subscribe to, provide or exchange products, property, information or services, or enabling or effecting, directly or indirectly, a commercial transaction.

The Regulations further includes circumstances where the personal data is used for direct marketing through:

a. sending of a catalogue through any medium addressed to a data subject;
b. displaying an advertisement on an online media site where a data subject is logged on using their personal data; or
c. sending an electronic message to a data subject about a sale, or other advertising material relating to a sale, using personal data provided by a data subject.

An exception to direct marketing restrictions is provided where the personal data is not used or disclosed to identify or target a particular recipient.

Personal data other than sensitive personal data is only permitted to be used for direct marketing where:

a. the data controller or data processor has collected the personal data directly from the data subject;
b. a data subject is notified that direct marketing is one of the purposes for which personal data is collected;
c. the data subject has consented to the use or disclosure of the personal data for the purpose of direct marketing;

d. the data controller or data processor provides a simplified opt-out mechanism for the data subject to request not to receive direct marketing communications; or
e. the data subject has not made an opt-out request.

The Cabinet Secretary in charge of information, communication and technology may, in consultation with the DPC, develop guidelines on the commercial use of personal data.

ONLINE PRIVACY

Kenyan law does not regulate online privacy. The Regulations have not prescribed any requirements or guidelines in regulating online privacy.

KEY CONTACTS

IKM Advocates
www.dlapiperafrica.com/en/kenya/

William Maema
Partner
IKM Advocates
T +254 20 2773 000
wmaema@ikm.co.ke

Imelda Anika
Senior Associate
IKM Advocates
T +254 722 898 393
ianika@ikm.co.ke

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

KOSOVO

Last modified 11 January 2024

LAW

The Law on Protection of Personal Data No.06/L-082 (“**LPPD**”) is the Kosovan law which entered into force and became applicable on 13 February 2019. The LPPD transposes the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (“**GDPR**”).

Scope of application

The LPPD has a wide scope of application. Namely, the LPPD applies to (Article 2):

- processing activities by private as well as public bodies;
- processing of personal data in diplomatic and consular offices, including any representative office of Kosovo abroad.

The LPPD has extraterritorial scope in that it applies to data controllers not established in Kosovo, which for the purposes of processing personal data make use of automatic or other equipment in Kosovo; nevertheless, the LPPD will not apply if such equipment is used only for transit purposes through the territory of Kosovo (Article 2(2)).

In addition to LPPD, in 2023 Kosovo has adopted Regulation no.02/2023 on Processing of Personal Data Obtained from Drone Use (“Regulation 02/2023”) which aims to define and establish specific responsibilities and measures related to processing of personal data by the drone owner or operator.

DEFINITIONS

Definition of Personal Data

“**Personal Data**” is defined as *“any information related to an identified or identifiable natural person (‘ data subject’).*"

An identifiable natural person is defined widely as any person *“who can be identified directly or indirectly, particularly by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.*

Definition of Sensitive Personal Data

“**Sensitive Personal Data**” is defined as “*personal data revealing ethnic or racial origin, political or philosophical views, religious affiliation, union membership or any data related to health condition or sexual life, any involvement in or removal from criminal or offence records retained in accordance with the law. Biometric characteristics are also considered sensitive personal data if the latter enable the identification of a data subject in relation with any of the abovementioned circumstances in this sub-paragraph. ”*

Genetic data, biometric data and data concerning health are also considered as sensitive category of personal data within the meaning of the LPPD.

NATIONAL DATA PROTECTION AUTHORITY

The competent national data protection authority in Kosovo is the Information and Privacy Agency (“**IPA**”) which is established as an independent agency, responsible for the supervision of implementation of the legislation on personal data protection, as well as access to public documents, in order to protect the rights and fundamental freedoms of natural persons in relation to the personal data processing and ensuring the guarantee of access to public documents.

IPA is divided into two organisational structures, namely (Article 58 (4)):

- access to public documents;
- protection of personal data.

IPA is charged with the following tasks (Article 64 (1)):

- supervision of the implementation of the LPPD;
- advising of public and private bodies on issues related to data protection;
- informing the public on issues and developments in the area of personal data protection;
- promotion and support of fundamental rights;
- deciding on complaints submitted by the data subjects;
- advising the Assembly, the Government and other institutions and bodies on legislative and administrative measures with regards to the protection of fundamental rights and freedoms of natural persons in terms of data processing;
- carrying out inspections with regards to the implementation of the LPPD;
- on its own initiative or upon request, providing opinions for public and private bodies, as well as publishing on any issues related to personal data protection.

REGISTRATION

Considering that the LPPD transposes the GDPR, same as the latter, it provides meticulous and protective measures to which the Controllers and the Processors must comply, and as such does not impose restrictive registration or notification requirements to be undertaken with the IPA. Accordingly, in general, LPPD does not contain mandatory provisions requiring registration of processing activities.

However, certain notification requirements apply in cases where a data protection impact assessment suggests a high risk without adequate protection measures (Article 36.1). Further, controllers or processors must report their appointed data protection officer to the IPA, where such appointment is required by law (Article 37.7). In the private sector, controllers or processors using biometric data for their activities must inform the IPA beforehand. This includes providing a detailed description of safety measures for processing biometric data (Article 83).

Additionally, controller and processor, including entities which process personal data based on the LPPD, are required to obtain the certification to perform work related to personal data (Article 43(1)). In practice, the certification procedure is not applicable in Kosovo, and its implementation is subject to the adoption of a sub-legal act (Article 43 (2)).

DATA PROTECTION OFFICERS

Controllers and Processors must appoint a data protection officer in the following cases (Article 37 (1)):

- The processing is carried out by a public authority or body, except in cases of courts acting in their judicial capacity;
- The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and / or their purpose, require regular and systematic monitoring of data subjects on a large scale;
- The core activities of the controller or the processor consist of processing, on a large scale, of sensitive personal data, and processing of personal data related to criminal convictions and offences.

A group of undertakings has the option to appoint a joint data protection officer, provided that the officer remains easily accessible to every entity within the group (Article 37.2). The appointment of a data protection officer is based on their professional knowledge and experience in data protection laws (Article 37.5).

The LPPD outlines the following tasks for data protection officers (Article 39.1):

i. Informs and advice controllers and / or processors on their obligations when processing personal data;
ii. Where required, provides advice on the data protection impact assessment and monitor its performance;
iii. Cooperate with IPA;
iv. Act as the contact point for the IPA on issues relating to processing of personal data.

COLLECTION & PROCESSING

LPPD adopts a wide definition of processing. Namely, processing includes *any operation or set of operations performed to personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction* (Article 3(1)(2)).

For the purposes of LPPD, data controller is defined as *any natural or legal person, public authority or other body which, alone or jointly with others, determines the purpose and means of personal data processing* (Article 3(1) (11)), whereas the processor is defined as *a natural or legal person, from public or private sector which processes personal data for and on behalf of the data controller* (Article 3(1) (14)).

When collecting and processing of personal data, Controllers must abide to the basic principles of data processing set forth in the LPPD. Namely, personal data must be collected and processed based on the following principles (Article 4):

- **Principle of lawfulness, justice and transparency**: personal data must be collected and processed in an impartial, lawful and transparent manner, without infringing the dignity of the data subjects.
- **Principle of purpose of limitation**: personal data must be collected and processed only for the specified, explicit and legitimate purposes and cannot be further processed in a manner which is incompatible with the stated purposes. However, in cases of further processing for archival purposes in the public interest, scientific or historical research, as well as statistical purposes, will not be considered to be incompatible with the initial purpose.
- **Principle of data minimisation:** the personal data should be adequate, relevant and limited to the purpose for which they are further collected or processed.
- **Principle of accuracy:** personal data should be kept accurate at all times, and kept up to date. In this line, every reasonable measure should be taken to ensure that inaccurate personal data are rectified or erased without delay.
- **Principle of storage limitation:** personal data may be stored insofar as necessary to achieve the purpose for which they are processed or collected; after which, the personal data should be erased, deleted, destroyed, blocked or anonymised, unless otherwise foreseen by another relevant law.
- **Principle of integrity and confidentiality:** personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by using appropriate technical and organisational measures;
- **Principle of accountability:** the controller is responsible for, and be able to demonstrate compliance with all the principles mentioned above.

Legal basis for processing of personal data (Article 5)

With reference to the list above, processing of personal data shall be considered lawful if one of the following criteria is met:

- The data subject has given consent for the processing of his/her personal data for one or more specific purposes;
- Processing is necessary for the performance of a contract to which the data subject is a contracting party or in order to take steps at the request of the data subject, prior to entering into a contract;

- Processing is necessary for compliance with a legal obligation to which the controller is subjected;
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller;
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child. This provision does not apply in cases where the processing is carried out by public authorities in the performance of their tasks.

Where the legal basis for processing is not based on the consent of the data subject or on the relevant legislation in force, in order to comply with the LPPD and lawfulness principle when processing personal data for purposes different from the initial purpose of the data collection, the following should be considered (Article 5(2)):

- Any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
- The context in which the personal data have been collected, in particular regarding the relationship between the data subjects and the controller;
- The nature of personal data being processed, especially in cases of processing of sensitive personal data or data related to criminal convictions;
- Possible consequences for the data subjects of the intended further processing;
- The existence of appropriate safeguards, which may include encryption or anonymisation.

Conditions for consent (Article 6)

Where the collection and processing of personal data is based on the consent of the data subject, the Controller must be able to demonstrate that the data subject has consented to process his/her personal data. In this line, when consent is given as a written declaration, the latter must be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language (Article 6(2)).

Processing of special categories of personal data (Article 8)

As a principle, LPPD prohibits the processing of special categories of personal data. Special categories of personal data within the meaning of the LPPD are used synonymously with sensitive categories of personal data.

Notwithstanding the above, exemptions to prohibition of processing of sensitive personal data include the following circumstances (Article 6(3)):

- The data subject has given his/her explicit consent to the processing of those personal data for one or more specific purposes, except where the relevant legislation in force provides that the general prohibition on processing of sensitive personal data cannot be lifted by the data subject;
- Processing is necessary for the purpose of carrying out obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, in so far as it is authorised by the relevant legislation in force or a collective agreement providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- Processing is necessary to protect the vital interests of the data subjects or other natural persons, where the data subject is physically or legally incapable of giving consent;
- If the data subject has made the sensitive personal data public, without limiting their use, in an evidenced or clear manner; processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity;
- Processing is necessary for reasons of substantial public interest, on the basis of the relevant legislation;
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of relevant legislation or pursuant to contracts with a health professional when such data are processed by a professional or under his/her responsibility subject to the obligation of

professional secrecy pursuant to respective legislation, established rules by national competent bodies or by another person subjected to professional secrecy;
- Processing is necessary for reasons of public interest in the area of public health, such as protection against serious cross-border threats to health, or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of the relevant legislation;
- Processing is necessary for archiving purposes in the public interest, as well as scientific or historical research purposes, or statistical purposes.

Except in cases where the data subject has made his/her sensitive personal data public, special categories of personal data should be protected in a special manner and be classified for the purpose of preventing unauthorised access or use (Article 8(4)). Classification of sensitive personal data refers to marking of personal data to indicate their sensitive nature (Article 3(1) (4)).

TRANSFER

In the context of transfer of personal data, the LPPD addresses two situations:

- Transfer of personal data to countries and international organisations which ensure an adequate level of data protection, and
- Transfer of personal data to countries and international organisations which do not provide adequate level of data protection.

With regards to the transfer of personal data to countries or international organisations that ensure proper and adequate level of data protection, as per a Decision adopted by the IPA, the list of countries and international organisations providing proper data protection, the latest being adopted on 13 September 2021 (“**the Decision**”) includes the following countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Iceland, Lichtenstein, Norway, and Switzerland.

Moreover, the LPPD expressly allows the IPA to rely on the decisions adopted by relevant EU bodies with regards to the transfer of personal data when drafting the list of approved countries providing adequate level of personal data protection (Article 46.2). Accordingly, based on the Decision, IPA considers some countries (including those outside the EU) ensuring proper level of data protection, in accordance with the EU Commission Decisions (Argentine, Andorra, Canada, Guernsey, Isle of Man, Jersey, Faroe Islands, Israel, New Zealand, Uruguay, Japan and United Kingdom).

With reference to the countries listed above, when transferring personal data, no special authorisation or permission is required from the IPA, provided the data subject is aware and informed that the personal data are being transferred, as required by the LPPD (Article 12.1.6).

In case of transfer to third parties located in other countries, such application will depend on whether such countries are included in the list of the IPA Decision or decisions of the EU Commission.

With regards to the transfer of personal data to international organisations, the Decision of the IPA does not specifically identify or address international organisations providing adequate level of personal data protection.

However, as a general principle, when deciding on the adequate level of data protection of another country or international organisation, the IPA shall firstly take account of the following elements (Article 47.1):

- The rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectorial, including public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another country or international organisation which apply within that country or international organisation, case-law, as well as effective and enforceable data subject right and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
- The existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data

protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities;
- The international commitments the third countries or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data;
- The type of personal data to be processed;
- The purpose and duration of the proposed processing;
- The legal arrangement in the country of origin and the recipient country, including the legal arrangement for protection of personal data of foreign citizens;
- The measures to secure personal data used in such countries and international organisations.

In addition, the above, in its decision-making process the IPA will particularly pay attention on (Article 47.2):

- Whether the personal data to be transferred will be or are used solely for the purpose of which they are being transferred, or whether the purpose may change only on the basis of a permission of the data controller supplying the data or on the basis of personal consent of the data subject;
- Whether the data subject has the possibility of determining the purpose for which his or her personal data will be used, to whom they are being transferred and the possibility of correcting or erasing inaccurate or out-dated personal data, unless this is prevented due to the secrecy of the procedure by binding international treaties;
- Whether the foreign data controller or data processor performs adequate organisational and technical procedures and measures to protect personal data;
- Whether there is an assigned contact person authorised to provide information to the data subject or to the IPA on the processing of personal data transferred;
- Whether the foreign data recipient may further transfer personal data, which may be done only on the condition that another foreign data recipient to whom personal data will be disclosed ensures adequate protection of personal data also for foreign citizens;
- Whether effective legal protection is ensured for data subjects whose personal data were or are being transferred.

In accordance with the above, it is safe to assume that international organisations fulfilling the listed criteria will be considered as providing adequate level of personal data protection. Additionally, international organisations deemed as providing adequate level of personal data protection by the EU Commission, may also be accepted by the IPA (Article 46.2).

SECURITY

LPPD contains general provisions when it comes to safety of processing of personal data. Security of processing of personal data refers to adopting appropriate organisational, technical and logical-technical procedures and measures in order to prevent any accidental, deliberate unauthorised destruction, disclosure, modification, etc. Implementing security measures is carried out by (Article 31 (1)):

- Pseudonymization and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The above measures of security are not sector-specific and apply to the processing of personal data in general.

In addition to implementing appropriate organizational, technical, and procedural measures for the secure processing of personal data, Regulation 02/2023 imposes specific measures on drone users to protect personal data, including (Article 8.1):

- Prohibiting unauthorized access to premises storing processed personal data.

- Restricting data access and prohibiting unauthorized use of archiving tools.
- Requiring authorization from licensed drone users for equipment commissioning and securing tools against unauthorized use.
- Mandating employees to lock computers, lockers, and offices containing personal data when leaving their workplace.
- Ensuring the protection of data from unauthorized access in the presence of non-employees.
- Prohibiting the display of personal data on screens in the presence of unauthorized persons.
- Restricting the removal of devices containing personal data from the office and ensuring data deletion or destruction in unsafe places.
- Prohibiting employees from recording or copying records without permission from the licensed user.
- Restricting the use of drone-collected data for purposes other than its intended collection, unless permitted by relevant personal data protection legislation.

BREACH NOTIFICATION

Breach notification to the IPA

LPPD foresees a mandatory breach notification to the IPA by data controllers not later than seventy-two (72) hours after becoming aware of the breach, unless the personal data breach is unlikely to risk the rights and freedoms of natural persons (Article 33 (1) (1)). When the data controller fails to report the breach after the 72 hours of becoming aware of it, the notification to IPA must also contain reasons on delayed notification.

With regards to the processors, the LPPD states that they should notify the breach to IPA *without undue delay* (Article 33 (2)), however a specific deadline as in the case of controllers is not provided.

Breach notification to the Data Subject

The data subject is notified on any breach resulting in a high risk to his/her rights and freedoms, without undue delay (Article 34 (1)). The obligation to communicate the breach to the data subject will not apply, provided the following conditions are met (Article 34 (3)):

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects (i.e. natural persons) is no longer likely to materialise;
- it would involve disproportionate effort, whereby, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

ENFORCEMENT

Filing a complaint at IPA

The data is subject is entitled to file a complaint with the IPA, while reserving the right to other administrative and judicial remedies (Article 52). IPA is obliged to notify the data subject on the decision of the complaint, as well as inform the data subject on the possibility of judicial remedy to uphold his/her rights with regards to violation of personal data (Article 52 (2)). However, if IPA fails to inform the data subject on a decision with regards to the complaint within three (3) months of its submission, the data subject shall be entitled to an effective judicial remedy (Article 53 (2)).

Filing a complaint against a Decision of the IPA

Every natural or legal person is entitled to file a complaint at the competent court against a binding decision of the IPA concerning them, by initiating an administrative dispute before the competent court (Article 53).

Right to an effective judicial remedy against a controller or processor

Without prejudice of the right of the data subjects to issue a complaint with the IPA, each data subject shall have the right to an effective judicial remedy in cases where he/she considers that the controllers or processors infringed the rights accorded by the LPPD, as a result of processing of his/her personal data.

With regards to filing complaints as described above, the data subject has the right to engage/mandate a non-profit body, organisation or association which has been established in accordance with the relevant law and is active in the field of personal data protection, to submit the complaint, represent and receive compensation on behalf of the data subject (Article 55 (1)).

Fines

Violations of provisions of LPPD are considered as minor offences/misdemeanours (i.e. *kundervajtje,* in Albanian) and are punishable by fines.

Fines for violation of provisions of LPPD, may be issued to legal persons, the authorised representative of the legal person or to the person exercising independent activities.

The severity of the fine depends on the identity of the offender, the nature of the violation and the extent of the violation.

IPA is authorised to issue fines to legal persons or to a natural person exercising independent activities, in the amount ranging from EUR 20,000 to EUR 40,000, if they fail to process personal data in accordance with LPPD, including but not limited to the following violations (Article 92 (1)):

- he/she processes personal data without any legal basis or without the consent of the data subject as provided by the LPPD;
- he/she entrusts an individual task relating to the processing of personal data to another person, without concluding a written contract as required by the LPPD;
- he/she processes sensitive personal data in violation of LPPD, or fails to provide the required protection to the sensitive personal data.

A fine ranging from EUR 2,000 to EUR 4,000 shall be imposed on the responsible/authorised representative of the legal person or to the person exercising independent activities (Article 92 (2)).

A fine ranging from EUR 1,000 to EUR 2,000 shall be imposed to the responsible person of a state body, in cases of minor offences with regards to personal data (Article 92 (3)).

A fine ranging from EUR 400.00 to EUR 1,000 shall be imposed to an individual, in cases of minor offences with regards to personal data (Article 92 (4)).

Serious and major violations of legal provisions

In cases where IPA finds a serious and grave violation of the provision of processing of personal data, it may impose a fine ranging from EUR 20,000 to EUR 40,000, or in cases of a company or enterprise it may impose a fine amounting to two percent (2%) of the general turnover of the company/enterprise for the previous fiscal year in compliance with the GDPR (Article 105).

ELECTRONIC MARKETING

LPPD applies to direct marketing activities and to automated decision-making including profiling. LPPD allows data controllers to use personal data obtained from publicly accessible sources or within the framework of lawful performance of activities for the

purposes of providing goods, services, employment or temporary performance of tasks, using postal services, telephone calls, e-mails or other telecommunication means (Article 73 (1)). With regards to direct marketing, the data controllers may only use the following personal data(Article 73 (2)):

- personal name
- permanent or temporary address
- telephone number
- e-mail
- fax number.

Other data may be processed only based on the data subject’s consent (Article 73 (2)).

A data subject is entitled to object at any time, the use of his/her personal data for the purposes of direct marketing (Article 74). The objection of the data subject must be submitted in writing, and within eight (8) days of receiving the objection, the controller must cease to use such personal data (Article 74 (1)).

ONLINE PRIVACY

There is no specific legislation with regards to on-line privacy (including cookies and location data). However, the LPPD considers location data and online identifiers as personal data (Article 3 (1) (1)). Accordingly, the processing data which fall within the definition of the LPPD, must be done in accordance with the provisions and principles of the LPPD.

Moreover, with reference to the location data, Law on Electronic Communications No.04/L-109 **(“LEC”)** stipulates that when location data are being processed, such data may be processed **only if they are made anonymous** *or* the users have given their consent for processing. In this line, Article 23 of LPPD provides the following: *“taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Law*" (Article 89 LEC).

KEY CONTACTS

Tashko Pustina Attorneys
tashkopustina.com/

Floran Pustina
Partner
Tashko Pustina Attorneys
T + 383 38 71 77 55
floran.pustina@tashkopustina.com

Mrika Gashi
Senior Associate
Tashko Pustina Attorneys
T + 383 49 61 36 65
mrika.gashi@tashkopustina.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

KUWAIT

Last modified 22 January 2024

LAW

To date, Kuwait does not have a specific personal data protection law. Previously, legislation such as Kuwait Law No. 20 of 2014, on Electronic Transactions (the “**E-Commerce Law**”), regulated privacy and data protection of private and public electronic records, signatures, documents, and payments. Whereas, Kuwait Law No. 63 of 2015, on Combating Cyber Crimes the (“**Cybercrime Law**”) imposed heavy penalties for illegal tampering with or acquisition of personal or governmental data or information.

However, the introduction of Decision No. 42 of 2021 on Data Privacy Protection Regulation (“**Data Protection Regulation**”) by the Communications and Telecommunications Regulatory Authority (“**CITRA**”), imposed obligations in relation to data protection on Telecommunication Services Providers and related industry sectors who collect, process, or store personal data, in whole or in part. The Data Protection Regulation describes the conditions for collecting and possessing personal data and the obligation of a service provider during the provision of the service or after the end thereof, in relation to the collection and processing of such data.

The introduction of the Data Protection Regulation has been a huge milestone since there was no dedicated data protection laws or regulations, and thus, reliance was placed on limited relevant legal provisions found under different legislation(s) such as the E-Commerce Law and Cybercrime Law. The Data Protection Regulation applies to all service providers irrespective of whether the data processing is undertaken inside or outside Kuwait, which requires that service providers inform users about how their data is collected, processed, and stored.

The Data Protection Regulation provides a wider ambit of the definition of “service provider” which ranges from traditional telecommunications service providers to anyone who operates a website, smart application or cloud computing service, collects or processes personal data or directs another party to do so on its behalf through information centers owned or used by them directly or indirectly. Furthermore, the Data Protection Regulation indicates that users have a right to withdraw their consent and, consequently, the service provider must delete / destroy the information provided by the user. However, the provisions of the Data Protection Regulation do not apply to natural persons who collect and process personal and family data; or security authorities for the purposes of controlling crimes and the prevention of threats related to public security.

Thus, the introduction of the Data Protection Regulation marks a significant milestone towards recognizing the importance that has been given to personal data in relation to Kuwait's legal scene. The Data Protection Regulation has brought a wide range of entities / sectors who are technically not TSP’s, to the extent that they are related to the field of telecommunication services, but own a website, an application, or provide cloud computing services etc., for which they collect data in some way from their users / customers.

Furthermore, CITRA has also issued, the Data Classification Policy (“**DCP**”), whereby entities dealing with large amounts of data can use as a guidance for data protection. The DCP classifies data into four separate categories to help in better decision making, regarding data access and processing in line with the data classification levels.

DEFINITIONS

Definition of personal data

Kuwaiti law does not define personal data. However, **personal data** is considered to include at least personal information about a person’s:

- Positional affairs
- Personal status
- Health status, or
- Elements of financial disclosures

These elements are undefined, but broadly construed to encompass any personal information relating to the specified data element.

Definition of sensitive personal data

Kuwaiti law does not define sensitive personal data.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in Kuwait.

REGISTRATION

Not required.

DATA PROTECTION OFFICERS

Not required.

COLLECTION & PROCESSING

The Regulation requires that prior to the provision of service, the service providers must:

- Provide all the information about the services to be provided and the terms of service in easy language both in English and Arabic;
- Clarify the purpose of collecting, and method of use of such data to the requester of service; and
- Obtain consent of the requester of service for collection and processing of data and his knowledge and acceptance of all conditions, obligations and provisions for data collection and processing.

Beside the Regulation, the E-Commerce Law includes a general obligation prohibiting Kuwaiti governmental bodies, agencies, public institutions, companies, non-governmental bodies, or employees thereof from collecting or processing any information in an illegal manner without the consent of the concerned person or his or her representative.

TRANSFER

The E-Commerce Law similarly includes a general obligation prohibiting Kuwaiti governmental bodies from transferring any information in an illegal manner without the consent of the concerned person or his or her representative.

SECURITY

No specific provisions.

BREACH NOTIFICATION

No specific provisions.

ENFORCEMENT

The Regulation does not provide specific penalties for breach of prescribed obligations but instead it prescribes to impose penalties and fine as per the CITRA Law, which lays down a range of punishments including imprisonment for a term from one to five years and fine ranging from five hundred Kuwaiti Dinars to twenty thousand Kuwaiti Dinars or a combination thereof.

Violations of the E-Commerce Law are punishable by a maximum of three years imprisonment, and fines of no less than KWD5, 000 (US$17,500) for anyone who discloses personal information without proper consent or a court order. The E-Commerce Law also provides for confiscation of tools, programs or devices used for unauthorized disclosure.

ELECTRONIC MARKETING

No specific provisions.

ONLINE PRIVACY

No specific provisions.

KEY CONTACTS

GLA & Company
www.glaco.com/

Ahmad Saleh
Senior Associate
GLA & Company
T +965 9220 3033
ahmad.saleh@glaco.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

KYRGYZSTAN

Last modified 29 January 2024

LAW

The Constitution of the Kyrgyz Republic prohibits collection, storage, use and dissemination of confidential information, private life information is not allowed without consent confidential/private life information subject.

More detailed regulation of personal data may be found in the Law of the Kyrgyz Republic on Personal Data No.58 dated 14 April 2008 ('The Law on Personal Data'), which entered into force on 18 April 2008. The most recent amendments were made to the Law on Personal Data on 29 November 2021. These amendments states that rules of processing of personal data for purposes of protection of the rights of participants in criminal proceedings is determined by the Cabinet of Ministers of the Kyrgyz Republic.

The Law on Personal Data is directed at legal regulation of work with personal data based on the standard international norms and principles according to the Constitution of the Kyrgyz Republic and laws of the Kyrgyz Republic is necessary first of all for assuring human personal rights and freedoms relating to the personal data gathering, processing and use.

The Law on Personal Data regulates relations arising at work with personal data, irrespective of the applied information processing means, except the work realization with the personal data, with its further transfer to the third persons.

Additional requirements to collection, use and transfer of personal data can be found in the following normative-legal acts:

- Procedure for Obtaining Consent of Personal Data Subject on Collection and Processing of its Personal Data, the Procedure and Form of Notification of Personal Data Subject on Transfer of their Personal Data to a Third Party approved by the Regulation of the Government of the Kyrgyz Republic dated 21 November 2017 # 759;

- Requirements for Ensuring the Security and Protection of Personal Data During their Processing in Personal Data Information Systems, the Implementation of Which Ensures the Established Levels of Protection of Personal Data approved by Regulation of the Government of the Kyrgyz Republic dated 21 November 2017 # 760.

The most recent amendments were made to the Law on Personal Data on 12 July 2022. These amendments include that part 5 and 6 of article 6 are stated as follows:

- at the request of the subject of personal data, the mode of public access to information (bibliographic directories, telephone and address books, private announcements, etc.) can be established. Exceptions are cases when information must be public in cases of administration of justice and execution of a judicial act, as well as in cases provided for by the laws of the Kyrgyz Republic in the field of electronic governance, national security, countering terrorism and corruption, operational-search activities and other cases determined by laws of the Kyrgyz Republic.
- from the moment of state registration of the death of the subject of personal data, the person is assigned the status of "deceased". The personal data of the deceased subject are subject to archiving and storage.[1]

[1] Law of the Kyrgyz Republic on Amendments to the Law of the Kyrgyz Republic on Personal Data dated July 12, 2022 No. 61

DEFINITIONS

The Law on Personal Data provides that information recorded on a material carrier relating to a particular person, which identifies a specific person or which could be used to identify a specific person, directly or indirectly, by reference to one or more factors related to biological, economic, cultural, civil or social identity shall qualify as '**personal data**'.

Personal data include:

- Biographical and identification data
- Personal characteristics
- Information on marital status
- Financial status
- Health data

There is no clear definition of Sensitive Personal Data. Under the provisions of the Law on Personal Data, all personal data is confidential. It should be noted that the Holder (Owner) of personal data (ie the data controller) and the data processor are obliged to ensure protection of personal data to prevent:

- Unauthorized access
- Blocking
- Transmission
- As well as its accidental or unauthorized destruction
- Alteration or loss
- Provide guarantees in respect of technical security measures and organizational measures regulating processing of personal data

However, confidentiality of personal data does not apply in cases of anonymisation or on request of the individual to which the personal data relates.

NATIONAL DATA PROTECTION AUTHORITY

The President of the Kyrgyz Republic by Decree No. 391 dated as of 14 September 2021 announced creation of the State Agency for Protection of Personal Data.

The Regulation on the Agency was adopted by the Resolution of the Cabinet of Ministers of the Kyrgyz Republic "On the State Agency for Personal Data Protection under the Cabinet of Ministers of the Kyrgyz Republic" dated December 22, 2021 № 325.

On January 10, 2022, the Agency was registered with the justice authorities.

The Agency consists of two departments:

- Department of legislative expertise of personal data;
- Department of ensuring protection and control of personal data processing.

Expert Council

In order to improve the personal data protection system within the Agency, an Expert Council was created, composed of independent experts and representatives of civil society in the field of cybersecurity and digital law.

The Regulation "On the Expert Council of the State Agency for Personal Data Protection under the Cabinet of Ministers of the Kyrgyz Republic" was approved by the Agency's Order No. 4-A dated April 22, 2022.

The purpose of the Expert Council is to make recommendations on amending the existing legislation and making proposals for the development of new normative legal acts and acts of the Agency.

REGISTRATION

The Law on Personal Data obliges Holders (Owners) of Personal Data Arrays to register with the competent state authority, however, to the best of our knowledge, none of Holders (Owners) of Personal Data Array has been registered to date, in particular, due to the fact that such regulator does not exist.

According to the Law on Personal Data within the registration procedure the following must be provided:

- Name and details of Holders (Owners) of Personal Data Arrays (ie data controller)
- Purposes and procedures of collection and processing of personal data
- Retention and terms of storage
- List of collected personal data
- Categories or groups of personal data bearers
- A source of collecting of personal data
- Procedure of notification of data subjects on collecting and possible transfer of personal data
- List of measures regarding the regime of confidentiality and safety of personal data
- Authorized person responsible for working with personal data
- Receiving party or category of receiving parties of personal data
- Proposed transfer of personal data outside of the Kyrgyz Republic

With regards to the registration obligation the procedure for registering holders (owners) of personal data arrays was approved.

Registration in the Register consists of three stages. During the first two stages, the holder fills in electronic forms to obtain a registration number in the Registry. During the third stage, the holder goes through the procedure for agreeing and registering lists of personal data for their collection, processing and storage as part of the implementation of their functions and purposes.

Registration of holders in the Register is carried out after authorization in the Register through the Unified Identification System through a cloud-based electronic signature of a legal entity. After filing the application, the holder receives a unique registration number in the Registry. Based on the results of registration in the Register, the holder receives the right to collect, process and store personal data in accordance with the legislation of the Kyrgyz Republic in the field of personal data.[1]

---

[1] The procedure for registering holders (owners) of personal data arrays, personal data arrays and lists of personal data in the Register of holders (owners) of personal data arrays, as well as its maintenance and publication approved by Decree of the Cabinet of Ministers of the Kyrgyz Republic dated November 18, 2022 No. 638

DATA PROTECTION OFFICERS

Under the Law on Personal Data, Holders (Owners) of personal data (ie the data controller) must indicate in its registration the name and contact details of the person that is responsible for the work with personal data. However, the Law on Personal Data does not contain any direct obligations to appoint a Data Protection Officer.

COLLECTION & PROCESSING

One of the basic principles of dealing with personal data is that personal data must be collected for accurately pre-defined, stated and legal purposes and must not be further processed in any manner incompatible with those purposes.

Processing of personal data is permitted in the following cases:

- The data subject has given its consent

- If it is necessary for public authorities, local authorities within their competence established by laws of the Kyrgyz Republic
- If it is necessary to achieve the legitimate interests of Holders (Owners)
- When implementation of these interests does not preclude the exercise of rights and freedoms of data subjects with regard to the processing of personal data
- When it is necessary to protect the interests of the data subject
- If personal data are processed solely for the purposes of journalism or for the purpose of artistic or literary works

TRANSFER

The Law on Personal Data allows transfer of personal data both within the country and abroad.

Transfer of personal data within the Kyrgyz Republic

- Data subject must be informed (in any form within a week)
- Personal data may be transferred without consent of the data subject in the following cases:
    - Extreme necessity in order to protect the interests of the data subject
    - Upon request of state authorities, local authorities, if the requested list of personal data fall under the competence of the requesting authority
    - Under any other case established by laws of the Kyrgyz Republic

Transfer of personal data outside the Kyrgyz Republic

- The cross-border transfer is carried out on the basis of an international treaty between the countries, under which the receiving party must provide adequate protection of the personal data
- Consent of the data subject has been obtained, or
- Personal data may be transferred to the countries that do not provide the adequate level of protection on certain conditions:
    - With consent of the data subject
    - If the transfer is necessary to protect the data subject's interests, or
    - If personal data are contained in the Public Personal Data database

When transferring personal data to the global information network (internet, etc) the Holder of the personal data (ie the data controller) transferring such data, shall provide the necessary means of protection with regard to the confidentiality of the information being transferred.

SECURITY

When processing personal data the Holder (Owner) of personal data (data controller) and processor shall:

- Prevent access of unauthorized persons to the equipment used for personal data processing (access control)
- Prevent unauthorized reading, copying, modification or removal of data media (control of data media use)
- Prevent unauthorized recording of personal data and alteration or destruction of stored personal data (entry control) and enable backdated determination of when, by whom and which personal data have been altered
- Ensure security of data processing systems, designed to transfer personal data irrespective of the data involved (control of data transmission means)
- Ensure that each user of a data processing system has only has access to the personal data which it is authorized to process (controlled access)
- Enable backdated determination of when, by whom and which personal data have been entered into the data processing system (input control)
- Prevent unauthorized reading, copying, alteration and destruction of personal data during the transmission and transportation of personal data (transport control)
- Ensure the confidentiality of the information in the course of personal data processing

BREACH NOTIFICATION

If the Holder (Owner) of personal data (data controller) transfers the personal data without consent of the data subject to a third party they must inform the data subject within a week.

ENFORCEMENT

Although the Law on Personal Data has been adopted, there is no enforcement practice of its provisions in place. However, since responsible agency has been appointed (State Agency for Protection of Personal Data), enforcement practice may change after the agency is fully operational.

ELECTRONIC MARKETING

Sending of electronic communications for advertising is generally subject to prior express consent of the recipient.

ONLINE PRIVACY

The Law on Electrical and Postal Communication establishes that all databases of telecommunication operators must be confidential and that telecom operators are obliged to keep communication data confidential.

KEY CONTACTS

Begaliev Kerim
Partner
Centil Law Firm
T +996 312 919780
kerim.b@centil.law

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

LAOS

Last modified 24 January 2024

LAW

In Laos, the comprehensive regulatory framework on data privacy focuses on data in its digital form – electronic data – and none other.

From 2012, Laos has introduced this framework by circulating relevant information only. This trend has accelerated since 2015 with the publication of the Law on Cyber Crime. Issues pertaining specifically to the protection of electronic data are regulated by the Law on Electronic Data Protection and the subsequent Instructions on the Implementation of the Law on Electronic Data Protection, as follows:

- Law on Electronic Transactions (2012)
- Law on Cyber Crime (2015)
- Decision on the Penalties of the Law on Cyber Crime (2017)
- Law on Electronic Data Protection (2017)
- Penal Code (2017)
- Instructions on the Implementation of the Law on Cyber Crime (2018)
- Instructions on the Implementation of the Law on Electronic Data Protection (2018)

In addition, for both professionals or non-professionals, the authorities have provided a series of guidelines of best practices for the use of software and hardware, social media platforms, and better protection of electronic data.

The two main pieces of regulation relating to data privacy are the Law on Electronic Data Protection and the Instructions on the Implementation of the Law on Electronic Data Protection.

DEFINITIONS

Definition of Personal Data

Article 3, Section 12 of the Law on Electronic Data Protection defines “personal data” to mean electronic data of an individual, legal entity, or organization.

Definition of Sensitive Personal Data

The Law on Electronic Data Protection aims to protect any type of electronic data. The law categorizes electronic data roughly into three types: (i) general data, (ii) sensitive data (a literal translation would be “specific data”), and (iii) prohibited data. Depending on its nature, personal data may fall under one these three categories. Accordingly, there is no “sensitive personal data” so to speak. Given this, personal data may fall under the category of sensitive data.

Sensitive data is information “that an individual, legal entity, or organization cannot access, use, or disclose if [they] have not received consent from the Information Owner, or the relevant organization” (Article 10).

A list of examples of sensitive data is provided in the Instructions on the Implementation of the Law on Electronic Data (2018), which includes “information on customers, financial information, CV, history of medical treatment, race, religion, project plan, budget plan, official servant secret, etc.” (Section 3). The list is not exhaustive, and there is no official guidance to anticipate what other data may be considered sensitive data apart from these examples.

NATIONAL DATA PROTECTION AUTHORITY

The Law on Electronic Data Protection (2017) originally delegated the Ministry of Post and Telecommunications (MPT) to handle matters related to the protection of electronic data. The MPT has now been renamed Ministry of Technology and Communication (MTC) and is the main administration in charge of issues pertaining to electronic data privacy across the country. The MTC is assisted by its departments located in each of the 17 provinces that compose Laos.

In its tasks to analyze and respond to digital issues and threats, the MPT was originally assisted by the Lao Computer Emergency Response Team (LaoCERT), which was established in 2012. LaoCERT is now a Division under direct supervision of the Department of Cyber Security in the MTC and is the agency on the front lines that receives reporting of security breaches from individuals or legal entities operating in Laos and / or complaints of offenses committed online.

REGISTRATION

There is no registration required for Data Protection Officers in Laos, or for any legal entities or individuals with a national data protection authority, as the case may be in other jurisdictions.

DATA PROTECTION OFFICERS

Under the Law on Electronic Data Protection, there is no data protection officer so to speak. The law introduces the idea that a team or an employee is required to supervise the protection of sensitive data; no information is provided on the duties and rights of such team or employee, or their scope of work. Moreover, the team or employee in charge of the protection of sensitive data is not required to register with any authority.

COLLECTION & PROCESSING

The collection of information is defined under the Instructions on the Implementation of the Law on Electronic Data Protection as “*the compiling of information in a database...for the convenience of access, monitoring, and use...*”.

The Law on Electronic Data Protection speaks literally of “administration” of data. Administration of electronic data refers to the management and arrangement of data, which includes the collection, copying, submission, receipt, maintenance, and destruction of electronic data. This administration of data is carried out by the Data Administrator, which is defined as an “individual, legal entity, or organization which has the duty to administrate electronic data, such as: a Ministry, an Internet Data Center, a Telecommunications Service Provider, an Internet Service Provider, or a Bank.” Apart from this definition, and the examples provided in the law, the Lao regulatory framework does not provide official guidance on who may or may not fall under the definition of Data Administrator.

By law, all data, general or sensitive, requires consent from the Information Owner to be collected. However, there is no information on how this consent may be collected.

Information Owner is defined as the individual, legal entity, or organization who / which is the owner of the electronic data. In this regard, the law does not necessarily identify the Information Owner as an individual only, or an individual who may be identified according to personal data that relates to him / her. The law only provides that the Information Owner is the entity that “owns” the information.

Sensitive data is more regulated as it requires the approval from the Information Owner for the access, use, and disclosure of sensitive data. At the time of the collection, the Information Owner must be informed of:

- the identity of the Data Administrator;
- the purpose of the collection of the information;

- the type of information that will be collected;
- the rights of the Information Owner, which include:
    - the right to amend the information provided;
    - the right to stop the sending or transfer of information to third parties;
    - the right to delete the information collected per request, or at the time that the purpose of the collection of the information expires.

Also, the Data Administrator and the Information Owner have the duty to ensure that the information provided is correct — it does not contravene local regulations, and does not affect the country’s socio-economic development, national stability, or social order.

TRANSFER

The Law on Electronic Data Protection provides that the transfer of data must abide by the following requirements:

- the Information Owner has given its consent for the transfer of the electronic data, and the individual or legal entity;
- transferring the electronic data ensures that the receiving entity can protect the electronic data properly;
- documents concerning important information, such as financial, banking, investment, and accounting information, must be encrypted;
- information which is transferred or submitted must not be distorted;
- the transfer must be in line with the agreement between the sender and the recipient; and
- submission or transfer of data must be stopped when the receiver of the data does not intend to receive the information anymore.

The law does not address whether the requirements above should be applied to all individuals or entities, or only to the Data Administrator.

In addition, the Law on Electronic Data Protection emphasizes that any individual, legal entity, or organization contemplating sending or transferring personal data or official data (pertaining to governmental bodies) out of Laos must obtain the consent of the Data Administrator, and ensure that such submission or transfer does not contravene the Lao laws without further details.

SECURITY

Generally, the Law on Electronic Data Protection requires the Data Administrator to ensure the following regarding the storage / maintenance of electronic data:

- there is a team or employee responsible for the administration of sensitive data;
- there is, among other things, an adequate system to store or use the data, and a data safeguard system to protect the data;
- there is a backup system for destroyed or deleted data;
- information is recorded by way of another appropriate method (e.g. paper, magnetic storage), and the appropriate measure is used to guarantee good maintenance;
- a risk assessment is conducted on the protection system at least once a year, and any failures uncovered during the inspection are corrected;
- access to the system is inspected, and protected from any intrusion, virus, or other risks;
- any adverse events that have occurred or are about to occur are immediately solved; and
- the information that is under the responsibility of the Data Administrator is protected.

BREACH NOTIFICATION

There is no mandatory breach notification in Laos under the Law on Electronic Data Protection. Individuals and legal entities facing a breach may make a notification, but to seek assistance and recommendations on how to solve the breach, and not for the sake of transparency.

However, in 2020, the Bank of Lao PDR issued the Decree on Consumer Protection Concerning Financial Services. Like the Law on Commercial Banks, enacted in 2018, the decree reiterates the importance of financial service providers (e.g. commercial banks) protecting their customer’s confidential information. However, unlike the Law on Commercial Banks, the Decree does mention a duty to maintain the confidentiality of “personal information”.

The Decree provides that in the event that information relating to customers is breached, the financial service provider has an obligation to record the incident and immediately notify the affected customers. No details are provided on what specifically must be recorded or notified. Likewise, the language used in the original document does not provide any assistance in interpreting the meaning of the term “affected.” The term for “affected” that is used in the Lao language version of the Decree is a term that is normally used to denote persons who have suffered negative consequences or damage from an act. In the event that the breach of information causes an important adverse impact, or if there is a large-scale breach, a report must be submitted to the Bank of Lao PDR. However, there is no definition of “important adverse impact” or “large scale breach.” Moreover, no specific sanction is provided for failing to submit the report.

The Law on Electronic Data Protection does not provide sanction for breach of the notification obligation. On the other hand, the Penal Code provides that any person disclosing the private confidential information of another person during the performance of their profession or duties, and who causes damages to the other person, will be liable to imprisonment of a term of three to six months and a fine between LAK 3 million (approx. USD 145) and LAK 10 million (approx. USD 480). However, Penal Code does not define “private confidential information”, nor does it state whether the disclosure of information must be intentional. To date, there is no official guidance clarifying whether the Penal Code applies to scenarios where customer data is breached as a result of a technical failure or other such incidents.

ENFORCEMENT

The enforcing authorities with regard to electronic data protection are:

- Ministry of Technology and Communications (MTC);
- Economic Police; and
- Lao People’s Court.

The Department of Cyber Security does not have by law the authority to issue fine or sanctions.

ELECTRONIC MARKETING

The Decision on Protection of Consumers Using Telecommunications and Internet Services (2020) regulates unsolicited commercial communications (e.g. phone calls or messages) to consumers, with the following restrictions:

- such calls and messages are prohibited from 8:00 to 17:00, Monday to Friday
- no more than 10 unsolicited commercial communications are allowed per month, per individual
- no more than two unsolicited commercial communications are allowed per day

The decision provides that any individual or legal entity intending to use unsolicited commercial communications for their goods or services must receive the consent of the telecommunications or internet service provider of the prospects they plan to call. The decision does not offer guidance on how the relevant service provider’s consent may be obtained. Rather, the decision requires the telecommunications and internet service providers to ensure that unsolicited communication commercials are made by authorized persons. In addition, the decision delegates these providers to monitor the distribution of unsolicited commercial messages, thereby ensuring that these limits are not breached.

Consumers who receive unsolicited commercial communications can file a complaint with the MPT and resolve subsequent disputes with the relevant service provider. The decision also notes that consumers can voice complaints or seek guidance via one of the following official hotlines:

- 1510 – Ministry of Industry and Commerce
- 1516 – Prime Minister’s Office

- 156 – National Assembly

The Ministry of Industry and Commerce’s website is also expected to become an available channel for complaints in the future.

ONLINE PRIVACY

As provided, the collection of data must receive the consent of the relevant Information Owner.

On the other hand, based on the main laws and regulations above, it is difficult to anticipate the category of data cookies and location data according to the ambiguous definitions of general data, sensitive data, and personal data.

KEY CONTACTS

Dino Santaniello
Head of Office
Tilleke & Gibbins Lao Co., Ltd
T +856 21 262 355
dino.s@tilleke.com

Saithong Rattana
Attorney-at-Law
Tilleke & Gibbins Lao Co., Ltd
T +856 21 262 355
saithong.r@tilleke.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

LATVIA

Last modified 11 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Personal Data Processing Law has been approved by the parliament and came into force on July 5, 2018. This law provides legal prerequisites for the implementation of the GDPR in Latvia and replaced the current Personal Data Protection Law.

DEFINITIONS

Personal data is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Personal Data Processing Law reproduces the definitions of Article 4 of GDPR, and generally uses the same terminology as the GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

According to The Personal Data Processing Law the Data State Inspectorate (DSI) has become an independent institution, however, still supervised by the government.

In addition to the tasks provided by the GDPR, The Personal Data Processing Law provides for the DSI to perform the following tasks:

- Verifying the compliance of the processing of personal data with the requirements of regulatory enactments when the controller is prohibited by law from providing information to the data subject, after receiving a relevant application from the data subject
- Investigating administrative offenses
- Participating, in accordance with its competence, in the drafting of laws and policies, and giving an opinion on draft laws and policy planning documents prepared by other institutions
- Providing opinions on the compliance of the personal data processing systems created by state and local government institutions with the requirements of regulatory enactments

- Monitoring the circulation of information society services in relation to the personal data protection
- monitoring the operation of credit information offices
- Issuing a license to credit information offices
- Cooperating with the supervisory authorities of foreign personal data protection, information disclosure and access control, and the prohibition of sending commercial communications
- Providing the transferring of a data subject's request for information concerning themselves to Eurojust and Europol
- Representing Latvia in international organizations and activities in the field of data protection
- Carrying out studies, analyzing situations, making recommendations, opinions and informing the public about current issues in the areas of its competence
- Performing other tasks prescribed by regulatory enactments

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Given that the GDPR does not provide for the registration of processing personal data, registries and systems will no longer exist. Pre-recorded data will remain as archived information about past activities.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale, or
- Its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have expert knowledge (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Personal Data Processing Law provides no derogation from the requirements of the GDPR regarding DPO. The Personal Data Processing Law provides the rules for examining an individual’s knowledge in data protection and obtaining the status of DPO. The Personal Data Processing Law allows data controllers and processors to appoint as a DPO any person who has the qualifications under the requirements of the GDPR.

The October 6, 2020 Cabinet Regulation No 620 “Data Protection Specialist Qualification Regulation” (**Regulation No 620**) determines in detail the application procedure, the content and procedure of the qualification examination and payment procedures for organizing the qualification exam. However, the qualification examination is not mandatory.

The Regulation No 620 does not set mandatory education requirements. A person who wishes to take the qualification exam, applies the Data State Inspectorate and pays the examination fee. After the person has passed the qualification exam, they are included in the list of the qualified DPOs maintained by the Data State Inspectorate and published on its website.

Regulation No 620 also provides for the maintenance of professional qualifications for DPOs who already have been included in DPOs' list. To maintain their professional qualifications, the DPOs must participate in the training in personal data protection or another field related to the performance of the DPO's duties.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous,*" and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to re-purpose personal data – *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. Necessary for entering into or performing a contract
b. Authorized by EU or Member State law
c. The data subject has given their explicit (*ie,* opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Personal Data Processing Law contains provisions on specific treatment related to the exercise of other fundamental rights of the individual, providing derogations relating to the data processing for archiving purposes, scientific or historical research purposes, statistical purposes, and the processing of national classified data.

The Personal Data Processing Law provides specific rules and exceptions regarding the journalistic, academic, artistic and literary processing of personal data. When processing data for these purposes, it is necessary to assess the balance between the right to privacy and freedom of expression.

The Personal Data Processing Law also provides for specific rules regarding the processing of data in the official publication. It states that the data published in the official publication is deleted by the publisher on the basis of a decision of the DSI or a decision confirming that such publication does not comply with the provisions of the GDPR.

The consent of a child for the use of information society services is deemed lawful where the child is at least 13 years old, meaning that Latvia has chosen the lowest threshold regarding the age of the child. Where the child is below the age of 13 years, such consent will be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules and standard contractual clauses. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. Explicit informed consent has been obtained
b. The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
d. The transfer is necessary for important reasons of public interest
e. The transfer is necessary for the establishment, exercise or defense of legal claims
f. The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
g. The transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The Personal Data Processing Law imposes a limitation period with respect to a data subject’s rights to information on the recipients or categories of recipients to whom the data have been transferred: the data subject has

the right to receive information about transfers within the last 2 years. The Personal Data Processing Law does not provide any other derogations or additional requirements to the GDPR regarding the transferring of the data.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

The Personal Data Processing Law does not provide any derogations or additional requirements to the GDPR regarding security.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Personal Data Processing Law does not provide any derogations or additional requirements to the GDPR regarding breach notification duties. The Data State Inspectorate has created a template for the data breach notification available on its webpage (only in Latvian).

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define undertaking and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of undertaking. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called look through liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent
- data subjects’ rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data
- Certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered material or non-material damage as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of non-material damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Enforcing the decisions provided for in Article 58 of the GDPR in relation to the imposition of a legal obligation, DSI will apply the Administrative Procedure Law. Under the Personal Data Processing Law, DSI is entitled to impose administrative sanctions to the legal entity governed by public law, e.g. state institutions. The liable official for unlawful activities with personal data and failure to comply with the obligations of the controller or processor may be punished up to EUR 1000.

The Personal Data Processing Law imposes a limitation period of 5 years for civil claims on the reimbursement of losses caused by the violations of the GDPR.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (eg, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Personal Data Protection Law does not specifically address (electronic) marketing. However the use of personal data for marketing purposes falls within the scope of the law. The provisions on electronic marketing are also included in the Law on Information Society Services, which requires prior express consent of the person before using his or her contact information (e.g. email address, phone number) for electronic marketing purposes. This is also stressed in the guidelines provided by DSI.

According to the provisions of the Law on Information Society Services no consent is required if the data has been obtained in the course of the sale of goods or provision of services, occurs for the same or similar goods or services, the recipient is able to decline easily and with no costs for the use of his or her personal data and the recipient has not previously declared that he or she does not want to be contacted.

The Electronic Communications Law contains procedures for submitting and reviewing complaints which states that the end user has the right to submit any complaints regarding the provision of the electronic communications services (thus also possibly any data protection issues), firstly, to the relevant electronic communications merchant and afterwards to the Public Utilities Commission (Article 44 of the Electronic Communications Law.

The Personal Data Processing Law does not provide any derogations or additional requirements to the GDPR regarding electronic marketing.

ONLINE PRIVACY

Specific issues of online privacy are regulated in the Electronic Communications Law and the Law on Information Society Services.

The Law on Information Society Services states that the storage of information received, including cookies or similar technologies, is permitted, provided that the consent of the person has been received after he or she has received clear and comprehensive information regarding the purpose of intended storage and data processing. Therefore, with regard to cookies Latvian law supports an opt in approach.

As to location data, the Electronic Communications Law permits the processing of location data only to ensure the provision of electronic communications services or if the express prior consent is obtained. The person whose location data is being processed has the right to revoke his or her consent or to suspend it at any time, notifying the relevant electronic communications merchant of this revocation or requested suspension.

The processing of location data for other purposes without the consent of a user or subscriber is permitted only if it is not possible to identify the person utilizing such location data or if the processing of location data is necessary for emergency services.

The Personal Data Processing Law does not provide any derogations or additional requirements to the GDPR regarding online privacy.

KEY CONTACTS

Sorainen
www.sorainen.com/

Ieva Andersone
Senior Associate, Head of Commercial & Regulatory Practice Group in Latvia
Sorainen
T +371 67 365 000
ieva.andersone@sorainen.com

Andis Burkevics
Senior Associate
Sorainen
T +371 67 365 007
andis.burkevics@sorainen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

LEBANON

Last modified 21 December 2022

LAW

Law No. 81/2018 relating to Electronic Transactions and Personal Data Law (the “**Law**”).

DEFINITIONS

Definition of Personal Data

Personal Data is defined as any information relating to an individual which helps identifying such individual, either directly or indirectly, including by way of comparing or combining information of multiple sources.

Definition of Sensitive Personal Data

The Law brings no definition of sensitive personal data per se. However, it states that the processing of personal data falling within specific categories shall only be processed under a license from the Ministry of Economy and Trade (exceptions apply).

The Law does not attribute a particular name for such category of data, simply listing specific data elements falling within the above defined category, as follows:

- those related to the external and internal security of the State, under the terms of a joint decision of the Ministers of National Defence and Interior and Municipalities;
- those related to criminal offences and judicial proceedings of various natures, under the terms of a decision by the Minister of Justice;
- those related to health, genetic identity, sexual life of individuals, under the terms of a decision of the Minister of Public Health.

NATIONAL DATA PROTECTION AUTHORITY

There is no National Data Protection Authority in Lebanon.

The Ministry of Economy and Trade is responsible for issuing permits and licenses for the processing of personal data when required under the Law.

REGISTRATION

Any person or entity wishing to process personal data must file a declaration before the Ministry of Economy and Trade obtaining a permit issued against receipt of such declaration, unless:

- when the data subject has agreed in advance to the processing of their personal data.
- when processed by public authorities, within their prerogatives;

- when processed by Non-Profit Organizations in relation to the members and clients thereof, within the scope of the normal and legal exercise of their functions;
- when processed for the purpose of keeping dedicated records required under the provisions of applicable laws and regulations, for the purpose of informing the public and which data can be accessed by any person having a legitimate interest;
- when processed by educational institutions in relation to their students and pupils, for educational or administrative purposes;
- when processed by institutions, commercial companies, trade unions, associations and liberal professionals in relation to their employees and members, within limits and for the needs of exercising their activities in a legal manner;
- when processed by commercial entities, associations, organizations, trade unions and liberal professionals in relation to their clients and customers, within limits and for the needs of exercising their activities in a legal manner.

DATA PROTECTION OFFICERS

The Law brings no definition of data protection officer.

COLLECTION & PROCESSING

Processing of Personal Data is defined as any action or set of actions performed on the data regardless of the medium used, including data collection, recording, organization, storage, adaptation, modification, extraction, reading, use, transmission, copy, dissemination, deletion, destruction or otherwise disposing of it.

The Law states that personal data shall be collected faithfully and for legitimate, specific, and explicit purposes. In addition, the data must: be appropriate; not exceed the set purposes; be correct and complete; and remain on a daily basis as relevant as possible.

Data controllers, or their representatives, have an obligation to inform data subjects of the following:

- the identity of the data controller or the identity of its representative;
- the purposes of the processing;
- the mandatory or optional nature of the raised questions;
- the consequences of non-response;
- the persons to whom the data is to be sent; and
- the right to access and correct information, as well as the means provided for the same.

TRANSFER

The Law is silent on cross-border data transfers.

SECURITY

The Law does not mandate specific technical security measures. Appropriate security standard is applicable.

The Law requires the data processor to take all measures, in light of the nature of the data and the risks resulting from processing thereof, in order to ensure the integrity and security of the data and to protect the same against being distorted, damaged or accessed by unauthorized persons.

BREACH NOTIFICATION

Not applicable.

ENFORCEMENT

Data subjects are entitled to resort to the competent courts, especially to the Judge of Expedite Matters, for matters related to enforcement of their rights under the Law.

There are no administrative enforcement actions.

Public prosecutor and/or data subjects can start legal proceeding for enforcement of the Law.

ELECTRONIC MARKETING

It is forbidden to communicate unsolicited marketing and advertising emails (SPAM) using a real person's name and address, unless that person has consented to such type of advertising, except for cases where the sender of the unsolicited advertisement has legally obtained the address of such individuals through a previous engagement with them.

The Law provides that any individual shall have the right to object to the processing of their personal data for legitimate reasons, including to the collection and processing of personal data for marketing/promotion purposes (exceptions apply).

ONLINE PRIVACY

The Law does not identify classes or types of personal data, while making no specific mention to cookies/cookie identifiers or location data. Qualification of online identifiers as personal data shall be assessed by local courts.

KEY CONTACTS

Alem & Associates
www.alemlaw.com/

Leila Laila
Partner, Head of IP, Franchising and Media
Alem & Associates
leila.laila@alemlaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

LESOTHO

Last modified 20 December 2021

LAW

The right to privacy is recognized and protected under the Constitution of the Kingdom of Lesotho.

Lesotho has established a Data Protection Act, 2013 (the DP Act). The DP Act provides principles for the regulation of the processing of any personal information in order to protect and reconcile the fundamental and competing values of personal information privacy.

DEFINITIONS

Definition of personal data

The DP Act defines personal data or information as being information about an identifiable individual that is recorded in any form, including:

- Information relating to the race, national or ethnic origin, religion, age or marital status of the individual
- Information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved
- Any identifying number, symbol or other particular assigned to the individual
- The address, fingerprints or blood type of the individual
- The name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual
- Correspondence sent to a data controller by the individual that is explicitly or implicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence
- The views or opinions of any other person about the individual

Definition of sensitive personal data

The DP Act defines sensitive personal information as any of the following:

- Genetic data, data related to children, data related to offenses, criminal sentences or security measure, biometric data as well as, if they are processed for what they reveal, personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, affiliation, trade-union membership, gender and data concerning health or sex life

- Any personal information otherwise considered by Lesotho law as presenting a major risk to the rights and interests of the data subject, in particular unlawful or arbitrary discrimination.

Section 29 prohibits a data controller from processing sensitive personal information, unless specifically permitted under the DP Act.

Section 36 contains general exemptions to the prohibition on processing sensitive personal information. These include instances where:

- Processing is carried out with prior parental consent where the data subject is a child and is subject to parental control in terms of the law
- The processing is necessary for the establishment, exercise or defense of a right or obligation in law
- Processing is necessary to comply with an obligation of international public law
- The Commission has granted authority in terms of section 37 for processing in the public interest, and appropriate guarantees have been put in place in law to protect the data subject’s privacy
- Processing is carried out with the consent of the data subject
- The information has deliberately been made public by the data subject

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Commission (Commission).

Part 2 of the DP Act provides for the establishment of a Data Protection Commission, an independent and administrative authority established to have oversight and control over the DP Act and the respective rights of information privacy.

The powers and duties of the Commission are set out in section 8 of the DP Act.

REGISTRATION

The DP Act (section 25(5)) requires that a data controller process personal information only upon notification to the Commission.

DATA PROTECTION OFFICERS

The DP Act (section 58) authorizes the head of a data controller to designate, by order, one or more officers or employees to be Data Protection Officers of that controller. In terms of that order, the Data Protection Officers may exercise, discharge or perform any of the power, duties or functions of the head of the data controller under this Act.

COLLECTION & PROCESSING

The DP Act defines processing as an operation or activity or any set of operations, whether or not by automatic means relating to any of the following:

- The collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use
- Dissemination by means of transmission, distribution or making available in any other form
- Merging, linking, as well as blocking, degradation, erasure, or destruction, of information

Under the DP Act (section 15(2)), personal information may only be processed where one of the following applies:

- The data subject provides explicit consent to the processing

- Processing is necessary for the conclusion or performance of a contract to which the data subject is a party
- Processing is necessary for compliance with a legal obligation to which the data controller is subject
- Processing is necessary to protect the legitimate interests of the data subject
- Processing is necessary for the proper performance of public law duty by a public body
- Processing is necessary for pursuing the legitimate interests of the data controller or of a third party to whom the information is supplied

Regarding the collection of data, the DP Act requires that a person shall collect personal information directly from the data subject, except where:

- The information is contained in a public record or has deliberately been made public by the data subject
- The data subject has consented to the collection of the information from another source
- Collection of the information from another source would not prejudice a legitimate interest of the data subject
- Collection of the information from another source is necessary:
  - To avoid prejudice to the maintenance or enforcement of the law and order
  - For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated
  - In the legitimate interests of national security
  - To maintain the legitimate interests of the data controller or of a third party to whom the information is supplied
- Compliance would prejudice a lawful purpose of the collection
- Compliance is not reasonably practicable in the circumstances of the particular case

TRANSFER

The DP Act distinguishes between the transfer of personal information to a recipient in a Member State of the South African Development Community (SADC) that has transposed the SADC data protection requirements and the transfer of personal information to a Member state that has not transposed the SADC data protection requirements or to a non-Member State.

Personal information shall only be transferred to recipients in a Member State that has transposed the SADC data protection requirements:

- Where the recipient establishes that the data is necessary for the performance of a task carried out in the public interest or pursuant to the lawful functions of a data controller, or
- Where the recipient establishes the necessity of having the data transferred and there is no reason to assume that the data subject's legitimate interests might be prejudiced by the transfer or the processing in the Member State

Further to the above, the DP Act requires that the controller make a provisional evaluation of the necessity for the transfer of the data. The recipient shall ensure that the necessity for the transfer of the data can be subsequently verified. The data controller shall ensure that the recipient shall process the personal information only for the purposes for which they were transferred.

Personal information may only be transferred to recipients, not SADC Member States subject to national law adopted pursuant to the SADC data protection requirements, if an adequate level of protection is ensured in the country of the recipient and the data is transferred solely to permit processing otherwise authorized to be undertaken by the controller.

The adequacy of the level of protection afforded by the relevant third country in question shall be assessed in the light of all the circumstances surrounding the relevant data transfer(s), particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing, the recipient’s country, the relevant laws in force in the third country and the professional rules and security measures which are complied with in that recipient’s country.

SECURITY

The DP Act regulates security measures on integrity of personal information processed by a data controller and security measures regarding information processed by an agent.

The DP Act (section 20) gives the data controller the duty to secure the integrity of personal information in its possession by taking appropriate measures to prevent the loss, damage to or unauthorised destruction of personal information and prevent the unlawful access to or processing of personal information. In order to give effect to this, the data controller should take the following reasonable measures:

- Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- Establish and maintain appropriate safeguards against the identified risks;
- Regularly verify that the safeguards are effectively implemented; and
- Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

The DP Act (section 21) states that any personal information processed by an agent should only be done with the knowledge and authorization of the data controller. Secondly the personal information should be treated as confidential unless the law or the performance of their duties requires disclosure. The following security measures are in place for information processed by an agent:

- A data controller should ensure that the agent processing the personal information establishes and maintains the security measures referred to in the DP Act.
- A written contract between the data controller and agent governs the processing of personal information by the agent.
- If the agent is not domiciled or does not have its principal place of business in Lesotho, the data controller should take reasonable steps to ensure that the agent complies with the laws relating to the protection of personal information of the territory in which the agent is domiciled.

BREACH NOTIFICATION

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an authorized person, the data controller, or any other third party processing personal information under the authority of a data controller, shall notify:

- The Commission, and

- The data subject, unless the identity of such data subject cannot be established

The notification shall be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the data controller’s information system.

The data controller, in terms of section 23(3), shall delay notification to the data subject where the Lesotho Mounted Police Service, the National Security Service or the Commission determines that notification will impede a criminal investigation.

The breach notification to a data subject shall be in writing and communicated to the data subject in one of the following ways:

- Mailed to the data subject’s last known physical or postal address

- Sent by email to the data subject’s last known email address

- Placed in a prominent position on the website of the party responsible for notification
- Published in the news media
- As may be directed by the commission

The notification is required to provide sufficient information to allow the data subject to take protective measures against potential consequences of the compromise, including, if known to the data controller, the identity of the unauthorized person who may have accessed or acquired the personal information.

Mandatory breach notification

See above.

ENFORCEMENT

The Commission is responsible for the enforcement of the DP Act.

The DP Act (section 49) also permits a data subject to institute a civil action for damages in a court having jurisdiction against a data controller for breach of any provision of this Act.

ELECTRONIC MARKETING

Under section 50 of the DP Act, direct marketing is defined in as a communication by whatever means of any advertising or marketing material which is directed to particular data subjects.

A data subject is entitled any time to require the data controller to cease, or not to begin, processing of personal data in respect of which he is the data subject for the purposes of direct marketing.

ONLINE PRIVACY

There are no sections of the DP Act which regulate privacy in relation to cookies and location data. These issues may be dealt with in future regulations, which the DP Act permits the Minister to make on the recommendations of the Commission.

KEY CONTACTS

Monique Jefferson
Director
T +27 11 302 0853
monique.jefferson@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

LIBERIA

Last modified 23 February 2024

LAW

Data Privacy Protection Laws.

DEFINITIONS

Definition of Personal Data

Personal Data is not defined by existing laws. Data is however, defined variously by different statutes and legal instrument in Liberia as follows:

- **Financial Intelligence Unit Act of 2012:** “**Data**" means: *representations, in any form, of information or concepts”.*
- **Central Bank of Liberia (“CBL”) E-Payment Regulation:** “**Data integrity**” means *“the assurance that information that is in-transit or in storage is not altered without authorization”*
- The ECOWAS Supplemental Act of which, Liberia is a signing member defines **personal data** as *“any information relating to an identified individual or who may be directly identifiable by reference to an identification number or one or several elements related to their physical, physiological, genetic, psychological, cultural, social, or economic identity”.* Accordingly, it can be concluded that that (i) cards numbers and (ii) account numbers from which a person can be directly identified qualify as sensitive personal information / data.

Definition of Sensitive Personal Data

There is no Liberian law that defines sensitive persona data.

NATIONAL DATA PROTECTION AUTHORITY

No specific national data protection agency or authority exists in Liberia, and besides a broad statement in the Liberian Constitution that *“no person shall be subjected to interference with his privacy of person, family, home or correspondence except by order of a court of competent jurisdiction”*, there is no dedicated privacy law whether of person or in respect of data, not to mention any dedicated data protection authority.

Admittedly, Liberia is a signatory to The ECOWAS Supplemental Act of which, requires member States, including Liberia, to establish National Data Authority within their jurisdiction. However, Liberia has not yet established such authority.

REGISTRATION

In terms of “Spatial Data”, Liberia Institute of Statistics and Geo-Information Services (LISGIS) is the public agency responsible for the collection of statistical and geographic information that are used to produce maps."

However, entity(ies) whose business requires the collection of data are required to register and receive the requisite permit / license from the government entity controlling / overseeing the sector in which the entity(ies) would be conducting business. Every permit / license issued by the requisite government authority is renewable.

DATA PROTECTION OFFICERS

There is no known or publicly designated Protection Officer, or Officers in Liberia. In the same vein, there is no law requiring the appointment or creation of such posts whether in public or private entities dealing with data.

COLLECTION & PROCESSING

Section 5.15.1 of the National Information and Communications Technology Policy of 2019 regulates the lawful processing of personal data. Its states that:

a. Personal data will be processed fairly and lawfully;
b. Personal data will be obtained only for one or more specified and lawful purposes, and will not be further processed in any manner incompatible with their purpose or those purposes;
c. Personal data will be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
d. Personal data will be accurate and where necessary, kept up to date;
e. Personal data processed for any lawful purpose or purposes will not be kept for longer than is necessary for that purpose or those purposes;
f. Appropriate technical and organizational measures will be taken against unauthorized or unlawful processing of personal data and the protection of children;
g. Data collectors will be required to disclose use of personal data to consumers.
h. Collected personal data will be rigorously protected from unauthorized access by any Parties.

Section 51(5) of the Telecommunication Act states that “Service providers shall ensure that customer information and customer communications are protected by security safeguards that are appropriate to their sensitivity”.

Section 3.1.1 of the 2017 AML / CFT Regulations for Financial Institutions in Liberia states that “financial institutions shall obtain and maintain documentary records for each client or customer to verify by reliable and independent source documents (such as a passport, a driver’s license, or national identification documents)”.

Section 3.1.7 of the 2017 AML / CFT Regulations for Financial Institutions in Liberia provides that the required KYC information must be collected before financial institutions establish any relationship with a person. That is, prior to opening a bank account or performing walk in transactional services for non-account holders

TRANSFER

The transfer of data out of Liberia is not specifically addressed by any Liberian law. However, Article 36 of the ECOWAS Act, as relied on in Liberia as a secondary source of law, restricts data controller from transferring personal data outside an ECOWAS country except said non-member ECOWAS country provides “*an adequate level of protection for privacy, freedoms and the fundamental rights of individuals in relation to the processing or possible processing of such data*”. In such a case, the data controller shall notify the Data Protection Authority, which is the Liberia Telecommunications Authority (LTA), prior to transferring any personal data.

Section 9(c) of the CBL E-Payment Regulation (though governing the Banking and Finance sector of Liberia, provides that “ *the system (used or being used) should be hosted locally to provide ease of support and guarantee data ownership; however, if the system is hosted in another jurisdiction, licensed institutions shall ensure that the information requested are provide promptly and that the CBL has unfettered access to reports generated by the system*”.

SECURITY

Section 9.1 of the CBL Regulations Concerning the Licensing and Operations of Electronic Payment Services in Liberia (“E-Payment Regulation”) provides as follows:

- *“All e-payment service providers shall ensure that personal information of customers obtained during the course of operations is used, disclosed, retained and protected as agreed”;* and
- *“They shall ensure the security, Integrity, Confidentiality and Availability of data and services by adopting prevailing international standard(s) as well as those prescribed by Central Bank of Liberia from time to time.”*

BREACH NOTIFICATION

There is generally no breach notification requirement, nor any dedicated agency or entity to which such notification must be made.

Mandatory breach notification

Whenever a private action is contemplated through the courts, it is mandatory that the accused is apprised of the matter in order to inform the prospective defendant of the allegation against him or her. This is usually accomplished through the issuance of the appropriate Writ issued by the court which is served upon the Defendant.

ENFORCEMENT

Enforcement is generally by a private right of action, but there are few administrative sanctions under some statutes and regulations, such as regulations governing the financial, insurance and telecommunications sectors, for violation of customer privacy by divulging confidential information without authorization.

ELECTRONIC MARKETING

Section 13.46(1) of the Liberia Electronics Transaction Law (2002) states that: *“a person who has access to any record, book, register, correspondence, information, document or other material in the course of performing a function under or for the purposes of this Law shall not disclose or permit or suffer to be disclosed such record, book, register, correspondence, information, document or other material to any other person”*. However, Section 13.46(2) of the Act provides that the above-quoted provision of Sub-section 1 does not apply to disclosure:

- Which is necessary for performing or assisting in the performance of a function under or for the purposes of this Law;
- For the purpose of any criminal proceedings in Liberia or elsewhere;
- For the purpose of complying with a requirement made under a rule of law with a view to instituting a criminal proceeding in Liberia or elsewhere; or
- Under the direction or order of a court.

ONLINE PRIVACY

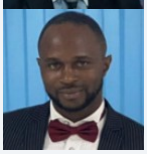
There are no specific provisions under Liberian laws relating to on-line privacy. However, data collectors are required to exercise the maximum protection of consumer’s protection and shall not disclose any information about a consumer to a third party except where (i) the institution is required by law to disclosed such information, or (ii) the disclosure is made with the expressed consent of the consumer. Data collectors are required to ensure the integrity and adequacy of their IT and Security system.

KEY CONTACTS

Heritage Partners & Associates Inc.
www.hpaliberia.com/

Cllr. Mark M.M. Marvey
Partner

Heritage Partners & Associates Inc.
T +231-777529389
mmarvey@hpaliberia.com



Atty. Beyan G. Mulbah
Associate
Heritage Partners & Associates Inc.
T +231-776428313
bmulbah@hpaliberia.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

LIBYA

Last modified 18 January 2024

LAW

Currently, there is no specific data protection law in Libya. However in recent years, Libya has witnessed a significant transformation in its legal framework with the introduction of pivotal legislation addressing data protection, cybercrime and electronic transactions. Law No. 5/2022 regarding Combating Cybercrime and Law No. 6/2022 concerning Electronic Transactions not only marks a significant step in adapting to the evolving digital landscape but also strengthens the overall data protection framework within the country. Articles 12 and 13 of the Constitution 2011 guarantee the right to a private life for citizens and the confidentiality of correspondence, telephonic conversations and other forms of communications except where required by a judicial warrant respectively. In other words, there is no detailed information concerning privacy systems in Libya that protect individuals when their data is processed. With regard to privacy protection, there are some provisions in the Libyan Penal Code (1953) that provide general protection for private correspondence and homes from any interference by others. These articles provide that the public servants who commit an offence against private correspondence will face imprisonment of no less than six months. Also, there are some articles in the Act No 4 (1990) on the National System for Information and Documentation, which governs the government’s collection of personal data for conducting research for social and economic reasons. This Act provides some provisions which require government entities to take some steps to protect the collected data, such as prohibiting the government from forcing individuals to give their data in order to conduct its research. However, these articles do not provide protection to personal data when individuals process their data. Also, the Central Bank of Libya regulated general criteria for protecting personal data which is available online. However, this is applicable to only Libyan banks.

DEFINITIONS

While Libyan Law does not explicitly provide a specific definition for personal data, the National Information Security and Safety Authority (NISSA) Policy Manual offers a comprehensive understanding of personal information, categorizing it into three distinct categories. It is worth noting however that NISSA policies are only binding on the public sector at the moment, rather than the private sector.

Definition of Confidential Data

Information that is classified as confidential or restricted includes data that can be catastrophic to one or more individuals and / or organizations if compromised or lost. Such information is frequently provided on a “need to know” basis and might include:

Personal data, including personally identifiable information such as Social Security or national identification numbers, passport numbers, credit card numbers, driver's license numbers, and medical records.

- Financial records, including financial account numbers such as checking or investment account numbers.
- Business material, such as documents or data that is unique or specific intellectual property.
- Legal data, including potential attorney-privileged material.

- Authentication data, including private cryptography keys, username password pairs.

Definition of Sensitive Data

Information that is classified as being of medium sensitivity includes files and data that would not have a severe impact on an individual and / or organization if lost or destroyed. Such information might include:

- Email, most of which can be deleted or distributed without causing a crisis (excluding mailboxes or email from individuals who are identified in the confidential classification).
- Documents and files that do not include confidential data.
- Anything that is not confidential. It can include most business data, because most files that are managed or used day-to-day can be classified as sensitive.

Definition of Public Data

Information that is classified as public includes data and files that are critical to business needs or operations. This classification can also include data that has deliberately been released to the public for their use, such as marketing material or press announcements. In addition, this classification can include data such as spam email messages sorted by an email service.

NATIONAL DATA PROTECTION AUTHORITY

There is no data protection authority as per Libyan Law. However, through an inclusive approach involving the government, private sector, academia, and civil society organizations, the National Information Security & Safety Authority (NISSA) was established to dynamically safeguard the confidentiality, integrity, availability, and resilience of information and communication technologies (ICT) infrastructure, resources, services, and data by providing high-quality information security and safety services. It is also positioned as an authoritative source for trusted information security expertise in the Libyan region.

Despite NISSA's policies on personal data protection, which are applicable only to Libyan state entities, private entities may consider these as indicators of the government's approach to data protection.

REGISTRATION

There are no registration requirements relating to personal data.

DATA PROTECTION OFFICERS

There is no data protection officer requirement as per Libyan Law.

COLLECTION & PROCESSING

In Law no. 6/2022 regarding Electronic Transactions, there are provisions relating to data collection and processing which are as follows:

‘Article 73

Any public entity and any authentication service provider may collect personal data directly from the person whom the data is collected about or from someone else, only after the explicit consent of this person and only for the purposes of issuing, maintaining, or facilitating a certificate.

Data may not be collected, processed, or used for any other purpose without the explicit consent of the person from whom the data was collected.

Article 74

Except for the previous article, obtaining, disclosing, providing, or processing personal data is legitimate if it is:

- *Necessary for the purpose of preventing or detecting a crime based on an official request from investigative bodies.*
- *Required or permitted under law or a court decision.*
- *For the assessment or collection of any tax or fee.*
- *To protect a vital urgent interest of the person whose data was collected.*

Article 75

Taking into account the previous article, the authentication service provider must follow appropriate procedures to ensure the confidentiality of the personal data in his custody while performing his duties. He may not disclose, transfer, declare, or publish such data for any purpose whatsoever without prior consent from the person whose data was collected.

Article 76

Any person who controls personal data by virtue of his work in electronic transactions must, before processing such data, inform the person from whom the data was collected by a special notification of the procedures he follows to protect personal data. These procedures must include identifying the person responsible for the processing, the nature of the data, the purpose of its processing, methods and locations of processing, and all the necessary information to ensure secure data processing.

Article 77

The authentication service provider must enable the person from whom personal data has been collected to access and update it. This right includes access to all personal data sites related to the person from whom the data was collected. Therefore, he must provide appropriate technological means to enable electronic access.’

Additionally, there are some articles in Law No. 4/1990 on the National System for Information and Documentation, which governs the government’s collection of personal data for conducting research for social and economic reasons. This Law provides some provisions which require government entities to take some steps to protect the collected data, such as prohibiting the government from forcing individuals to give their data in order to conduct its research. However, these articles do not provide protection to personal data when individuals process their data. Also, the Central Bank of Libya regulated general criteria for protecting personal data which is available online. However, this is applicable to only Libyan banks.

TRANSFER

There are no provisions relating to internal data transfer. However, there are provisions relating to international data transfer which are specified in article 78 of Law no.6/2022 which states:

‘Article 78

If necessary to transfer personal data outside of Libya, due consideration must be given to an appropriate level of protection, specifically:

1. *The nature of the personal data.*
2. *The source of the information included in the data.*
3. *The purposes for which the data is to be processed and its duration.*
4. *The country to which the data is being transferred, its international commitments, and the applicable law therein.*
5. *The relevant rules in that country.*
6. *The security measures taken to protect the data in that country.’*

SECURITY

Not applicable.

BREACH NOTIFICATION

There is no breach notification requirement in Libya.

ENFORCEMENT

It should be noted that recently, the Libyan House of Representatives enacted Law No.5 2022 concerning Combating Cyber Crimes in September 2022. In accordance with this law cybercrime is defined as “*every act committed through the use of computer systems, the international information network, or other information technology means in violation of the provisions of this law.* ”

This law has brought in some form of enforcement regarding breaches of copyright, with fines and prison sentences to be enacted in such a case. The sentence for copyright infringement is a prison sentence of no less than one year, and a fine of no less than 1,000 Dinars.

Furthermore, Law no.6/2022 regarding Electronic Transactions has also bought in some enforcement procedures relating to data protection. Article 79 states ‘*Entities collecting personal data according to Article 73 of this law are prohibited from sending electronic documents to the person from whom the data was collected if he explicitly refuses to accept them.*

Processing of personal data by the person who collected it is not allowed if he explicitly refuses to accept it. Additionally, processing is not allowed if it causes harm to the individuals from whom the data was collected, or infringes upon their rights or freedoms. The data may also not be used for any other purposes than those agreed upon unless consent is obtained from the data owner.’

Articles 81-84 of this law state:

'Article 81

Without prejudice to any stricter penalty stipulated by the Penal Code or any other law, anyone who commits any of the acts stipulated in Articles 79 …. of this law shall be punished with imprisonment for a period not less than one year and a fine of not less than three thousand dinars and not exceeding ten thousand dinars.

The penalty will be imprisonment and a fine of not less than ten thousand dinars if these acts were committed to disrupt electronic transactions related to the government or military or security institutions or banks.

Article 82

Without prejudice to the individual criminal liability of the perpetrator of the crime, the legal representative of the legal person shall be punished with the same penalties prescribed for the acts committed in violation of the provisions of this law, if it is proven that his failure to perform his duties contributed to the occurrence of the crime.

The legal person shall be jointly responsible for any financial penalties or compensations if the crime was committed on his behalf or in his name or for his benefit.

Article 83

Without prejudice to any stricter penalty stipulated by the Penal Code or any other law, anyone who exploits the weakness or ignorance of a person in electronic operations by compelling him to commit, presently or in the future, in any form, shall be punished with imprisonment for a period not less than one year and a fine not less than five thousand dinars and not exceeding ten thousand dinars, provided that it is proven from the circumstances that this person is unable to distinguish the dimensions of his commitments and obligations.

Article 84

Without prejudice to the rights of bona fide third parties, in all cases, the devices, programs, or means used in committing any of the crimes stipulated in this law or the funds obtained from them shall be confiscated.

It also provides for the closure of the shop or the site where any of these crimes are committed and the cancellation of its license if the crime was committed with the owner's knowledge.

The closure is either complete or for the period determined by the court.'

ELECTRONIC MARKETING

There is no specific law governing electronic marketing.

ONLINE PRIVACY

There is no specific online privacy legislation.

KEY CONTACTS

Abdou Law Firm
www.abdoulawfirm.com/

Dr Majdi Abdou
Founding Partner
Abdou Law Firm
T +218213610799
majdi.abdou@abdoulawfirm.com

Mohanad Hussein
Managing Partner
Abdou Law Firm
T +218213600028
mohanad.hussein@abdoulawfirm.com

Maram Bayou
Associate
Abdou Law Firm
maram.bayou@abdoulawfirm.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

LITHUANIA

Last modified 18 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The implementation of the GDPR has been achieved in the Republic of Lithuania. The Law on Legal Protection of Personal Data (hereinafter ‘Data Protection Law’) has been in force since July 16, 2018.

The Data Protection Law replaced the previous Law on Legal Protection of Personal Data which implemented the EU Data Protection Directive (Directive 95/46/EC).

DEFINITIONS

Personal data is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Data Protection Law refers to the definitions provided by the GDPR. Only two definitions: ‘direct marketing’ and ‘institutions and authorities’ are defined differently in the Data Protection Law.

Under the Data Protection Law, 'direct marketing' means any activity consisting of offering goods or services or asking opinion on the goods or services offered, by post, telephone or other direct means.

'Institutions and authorities' means state and municipal institutions and authorities, enterprises and public institutions, financed from state or municipal budgets and state monetary funds and authorized by the Law on Public Administration of the Republic of Lithuania to perform public administration activities or to provide public or administrative services to persons or to perform other public functions.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

There are two supervisory authorities in Lithuania: the State Data Protection Inspectorate and the Inspector of Journalist Ethics. The State Data Protection Inspectorate is responsible for monitoring the application of the GDPR and the Data Protection Law as well as ensuring these acts are applied, except where it is within the competence of the Journalist Ethics Officer. The Journalist Ethics Officer performs the same functions where the personal data is processed for

journalistic purposes and for academic, artistic or literary expression, except for tasks and powers listed in Article 57(1) (j) to (l) and (n) to (t), Article 58(1) (b) to (c), Article 58(2) (e), (g), (h) and (j), and Article 58(3) (a), (c) and (e) to (j) of the GDPR.

In addition to the tasks established in the GDPR, the Data Protection Law authorizes the State Data Protection Inspectorate to perform the following tasks:

- To provide advice to data subjects, data controllers and processors on the protection of personal data and privacy protection, and also to develop methodological recommendations for the protection of personal data and to publish them publicly on their website
- To cooperate with personal data protection supervisory authorities of other countries, European Union institutions and international organizations and to take part in their activities
- To participate in the formation of state policy in the field of personal data protection and to implement it
- To implement the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and its Protocols
- To perform other functions specified in the Data Protection Law and other legal acts

In addition to the powers established in the GDPR, the Data Protection Law authorizes the State Data Protection Inspectorate to:

- Receive all necessary information, copies of documents and duplicates, and copies of the data from the data controllers and data processors, state and municipal institutions and bodies, other legal and natural persons; as well as access to all data and documents which are necessary for the execution of tasks and functions of the State Data Protection Inspectorate
- During the investigation of the infringements to enter the premises of the person or entity which is subject to the inspection and to exercise similar actions with respect to related persons or entities
- Participate in meetings of the Parliament, the Government, and other state institutions when issues related to the protection of personal data or privacy are being considered
- Invite experts and consultants, to form working groups on examination of processing or protection of personal data, preparation of personal data protection documents and to deal with other issues which fall under the competence of the State Data Protection Inspectorate
- Provide recommendations and instructions to data controllers, data processors and other legal or natural persons regarding the processing of personal data or the protection of privacy
- Exchange information with other countries' personal data protection supervisory authorities and international organizations to the extent necessary for their functions
- Participate in court hearings when infringements of international, European Union or national law provisions on personal data protection issues are being considered
- Use technical measures during the investigation of infringements
- Receive oral and written explanations from legal entities and natural persons during the infringement proceedings and to demand that they arrive to provide explanations to the premises of the State Data Protection Inspectorate
- Use the information held by the State Data Protection Inspectorate, including personal data obtained during the investigation of infringements or received by the State Data Protection Inspectorate for other functions
- Involve police officers in order to ensure the possible use of violence and in order to maintain public order
- Perform other functions specified in the law

More information and contact details of supervisory authorities are available at:

- State Data Protection Inspectorate
- Inspector of Journalist Ethics

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Given that the GDPR does not provide for the registration of data processing activities, registries and related systems no longer exist.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale
- Its core activities consist of processing sensitive personal data on a large scale

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Data Protection Law does not determine any derogations from the requirements which are set in the GDPR regarding data protection officers.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous,*" and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent

- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to re-purpose personal data – *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)

- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg*, commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate compelling legitimate grounds for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. Necessary for entering into or performing a contract
b. Authorized by EU or Member State law
c. The data subject has given their explicit (*ie,* opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Data Protection Law contains provisions on specific conditions related to the processing of national identification number.

Article 3 of the Data Protection Law determines particularities of the processing of the personal code:

- Personal code can be processed if there is at least one of the conditions for the lawfulness of the processing of personal data referred to in Article 6(1) of Regulation (EU) 2016/679
- It is forbidden to disseminate the personal code
- It is forbidden to process personal code for direct marketing purposes

The Data Protection Law provides specific rules and exceptions regarding processing of personal data for journalistic, academic, artistic and literary purposes. When processing data for these purposes, Articles 8, 12-23, 25, 30, 33-39, 41-50 and 88-91 of the GDPR shall not be applicable.

The Data Protection Law also provides specific rules regarding processing of personal data in the employment context:

- It is forbidden to process the personal data of candidates and employees related to convictions and offences committed by the candidate or employee, unless such personal data are necessary to verify that a person meets the requirements of law or implementing legislation for the purpose of performing work or other duties.
- The data controller may collect personal data relating to qualifications, professional skills and business characteristics of a candidate applying for job from a former employer by duly informing the candidate, and from the existing employer by receiving consent of the candidate.
- The processing of video or audio data in the workplace and at the data controller's premises or in the areas where employees work, in the processing of personal data relating to the monitoring of employees' behavior, employees must be informed of such processing of their personal data in writing or by any other means which allow to prove the fact that the information referred to in Article 13(1) and (2) of Regulation (EU) 2016/679 has been provided.

The consent of a child for the use of information society services is deemed lawful where the child is at least 14 years old. Where the child is below the age of 14 years, such consent will be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility for the child.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules, standard contractual clauses. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. Explicit informed consent has been obtained;
b. The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. The transfer is necessary for important reasons of public interest;
e. The transfer is necessary for the establishment, exercise or defense of legal claims;
f. The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. The transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The Data Protection Law provides that the State Data Protection Inspectorate must issue an authorization for the transfer of personal data to a third country or an international organization under Art. 46(3) of the GDPR or a substantiated written refusal to issue such an authorization within a maximum of 20 working days.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However, the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

The Data Protection Law does not provide any derogations or additional requirements to the GDPR regarding security.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Data Protection Law does not provide any derogations or additional requirements to the GDPR regarding breach notification duties.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions

often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent;
- Data subjects’ rights;
- International transfer restrictions;
- Any obligations imposed by Member State law for special cases such as processing employee data; and
- Certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations;
- Obligations of certification bodies; and
- Obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The Data Protection Law sets out administrative fines which can be imposed on public institutions. The State Data Protection Inspectorate has the right to impose an administrative fine:

- Up to 0.5% of the annual budget of the institution in the current year or of the total annual revenue received in the previous year but not exceeding EUR 30000 for breach of the provisions referred to in the paragraphs a-c of Article 83(4) of the GDPR
- Up to 1% of the annual budget of the institution in the current year or of the total annual revenue received in the previous year, but not exceeding EUR 60000, for breach of the provisions referred to in the paragraphs a-e of Article 83(5) and Article 83(6) of the GDPR
- When a public authority or body carries on commercial business, according to sections 4-6 of Article 83 of the GDPR

The statute of limitation is two years from when the offence has been committed, and in case of continued offences, within two years after the offence has been identified.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Electronic marketing to individuals in Lithuania must only be conducted in accordance with the Data Protection Law, the Electronic Communications Law and the Law on Advertising of the Republic of Lithuania (Advertising Law).

General requirements for direct marketing:

- The recipient (either natural person or legal person) has given his prior consent (under Lithuanian law, an opt-in principle applies, ie, the customer should actively express his willingness to receive commercial communication)
- The recipient’s consent must be obtained separately from other terms of the contract between the parties
- Consent cannot be obtained in the standard terms presented to the recipient (eg, “by accepting these terms you agree to receive our commercial communication to the email provided to us”). The consent must stand separately from other contractual terms, so that the data subject has an actual possibility to choose whether he or she wants to receive commercial communication from the company or not
- The company must ensure that recipients have been given a clear, free-of-charge and easily realizable possibility not to give their consent or refuse giving their consent for the use of this data for the above-mentioned purposes at the time of collection of the data and, if initially the recipient has not objected against such use of the data, at the time of each offer

No direct marketing should be carried out where the contact has requested not to receive unsolicited direct marketing.

Exemption: if the company has obtained electronic contact details in the process of selling a product or a service, it is allowed to use these details for direct marketing provided that the recipient (either natural person or legal person) is given an opportunity to refuse such marketing; this opportunity shall continue to be offered with each message.

Additional requirements under the Advertising Law:

- Direct marketing must be clearly recognizable as a commercial communication
- The person on behalf of whom this commercial communication is distributed must be clearly identified
- The content of the offer and conditions regarding receiving of the service must be formulated clearly and precisely

Each marketing communication is a separate violation, for which a penalty of up to EUR 3,000 may be imposed.

As mentioned above, the Data Protection Law provides a definition of direct marketing and prohibits the processing of personal code for direct marketing purposes.

ONLINE PRIVACY

Traffic Data

Traffic Data held by a public electronic communications services provider must be erased or anonymized when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

- It is being used to provide a value added service
- consent has been given for the retention of the Traffic Data
- It is required for investigation of a grave crime

Traffic Data can only be processed by a CSP for:

- The management of business needs, such as billing or traffic
- Dealing with customer enquiries
- The prevention of fraud
- The provision of a value added service

Cookies

The use of cookies is permitted only if approved by the user (under Lithuanian law, an opt-in principle applies). However, consent is not required for cookies used for website technical structure and for cookies used for showing website content. Consent is not required for session ID cookies and for so called 'shopping basket' cookies (these exceptions do not apply if such cookies are used for collecting statistical information on use of the website).

Clear and exhaustive information on use of cookies, including information about the purpose of cookie related data processing, must be provided. This information should be provided in the privacy policy of the website. Consent to the terms of the website’s privacy policy or terms of use containing the information on use of cookies is considered insufficient. Consent though web browser settings may be considered adequate only if the browser settings allow choosing what cookies may be used and for what purposes. However, considering the nature of currently used web browsers consent through web browser settings is not considered appropriate under Lithuanian law.

Location data

Processing of location data triggers personal data processing laws. The data controller must have a legitimate basis for such personal data processing (*eg*, the data subject has given his consent; a contract to which the data subject is party is being concluded or performed; it is a legal obligation of the data controller under laws to process personal data; processing is necessary in order to protect vital interests of the data subject; etc.).

The Data Protection Law does not provide any derogations or additional requirements to the GDPR regarding online privacy.

KEY CONTACTS

Sorainen
www.sorainen.com/

Stasys Drazdauskas
Counsel
Sorainen
T +370 52 685 040
stasys.drazdauskas@sorainen.com

Irma Kirklytė
Counsel
Sorainen
T +370 52 685 040
irma.kirklyte@sorainen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

LUXEMBOURG

Last modified 12 January 2023

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

In addition to the GDPR, the legal regime of data protection in Luxembourg is completed by the following laws:

- the Law of August 1, 2018 on the organization of the National Data Protection Commission (CNPD) and the general data protection framework. It has repealed the previous Law on Data Protection (amended Law of August 2, 2002) and completes the GDPR at the national level. Most of all it gives the framework for the CNPD's organization, composition and powers under the GDPR and the applicable national law;

- the Law of August 1, 2018 on the protection of individuals with regard to the processing of personal data in criminal matters as well as in matters of national security, implementing Directive (EU) 2016/680; and

- the amended Law of May 30, 2005 on data protection and electronic communications governs the protection of personal data in the field of telecommunications and electronic communications, implementing the Directive 2002 /58/EC.

It is also to be noted that Article L. 261-1(1) of the Labour Code provides specific regulations concerning employer workplace surveillance.

Along with several CNPD’s recommendations, the Law of July 17, 2020 introducing a series of measures to combat the Covid-19 pandemic as amended provides a legal framework on the processing of personal data in the context of the COVID-19 crisis.

DEFINITIONS

Personal data is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definition of personal data has not been amended by applicable law. GDPR definitions apply.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Commission Nationale pour la Protection des Données (CNPD)
15, Boulevard du Jazz, L-4370 Belvaux

T +352 26 10 60 1
F +352 26 10 60 29.

The CNPD is in charge of monitoring and checking that the data are processed in accordance with the GDPR, as well as the Law of August 1, 2018 on the organization of the National Data Protection Commission, the Law of August 1, 2018 on the protection of individuals with regard to the processing of personal data in criminal matters and in matters of national security, and any applicable legislation that may include specific personal data protection provisions.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

No specific provisions in the applicable law.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale
- Its core activities consist of processing sensitive personal data on a large scale

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have expert knowledge (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested

- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

Article 65(1) of the Law of August 1, 2018 on the organization of the National Data Protection Commission provides for a specific obligation to appoint a DPO in the context of processing of personal data for scientific or historical research purposes or statistical purposes. Such appointment must be made in accordance with the nature, scope, context and purposes of the processing, as well as the risks for the rights and freedoms of the relevant data subjects. In this regard, if the data controller elects not to appoint a DPO, it must then formally document and justify why it chose not to appoint a DPO, for each project involving a processing of personal data for scientific or historical research purposes or statistical purposes.

Article 64 of the Law of August 1, 2018 on the organization of the National Data Protection Commission provides that the same applies to processing of special categories of personal data for the purposes defined in Article 9(2)(j) GDPR (*ie,* processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes).

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous,*" and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)

- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to re-purpose personal data – *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. Necessary for entering into or performing a contract
b. Authorized by EU or Member State law
c. The data subject has given their explicit (*ie,* opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The Law of August 1, 2018 on the organization of the National Data Protection Commission provides specific regulations concerning the processing of personal data for the purposes of the surveillance of employees at the workplace by the employer (thus modifying Article L. 261-1(1) of the Labor Code). In this respect, the employer must comply with a certain set of obligations, in addition to its general obligations as a data controller under the GDPR.

Notably, the employer must inform certain employee representation bodies of the contemplated processing of personal data. This information must contain a detailed description of the purposes of the contemplated processing, the means of implementation of the surveillance, and the retention policy for the personal data concerned.

When employees or their representation bodies are informed that their personal data may be processed for surveillance purposes, they may ask the CNPD for a preliminary opinion on the compliance of such surveillance project with applicable data protection legislation. The employer may not begin surveillance until the CNPD hands out its decision.

When surveillance has already been put it place by the employer, employees have a right to file a complaint with the CNPD if they believe that processing does not comply with applicable data protection legislation. Filing such complaint may not be held as a grounds for dismissal.

Finally, the Law of August, 1 2018 on the organization of the National Data Protection Commission provides three specific provisions complementing the GDPR in matters left to Member State discretion.

1. Processing of personal data for the sole purpose of journalism, university research, art or literature

This processing is not subject to:

- Prohibitions on processing special categories of personal data set out under Article 9(1) GDPR
- Limitations applicable to processing of personal data relating to criminal convictions and offences (Article 10, GDPR):
  - Provided such processing concerns data made publicly available (in an obvious fashion) by the data subject
  - If the data are directly connected to the public life of the data subject
  - If the data are directly connected to an event in which the data subject has willingly become involved
- Obligations imposed on the data controller in case of a transfer of personal data to third countries or international organizations (Chapter V, GDPR)
- The obligation of the data controller to provide information to the data subject where personal data are collected from the data subject (Article 13, GDPR), when providing such information would jeopardize the collection of personal data from such data subject
- The obligation of the data controller to provide information to the data subject where personal data have not been obtained from the data subject (Article 14, GDPR), when providing such information would jeopardize either the collection of personal data, a publication project, making such personal data available to the public in any way whatsoever or would provide indications as to the source of information
- The obligation to provide the data subject with the right of access to his or her personal data. Such right is postponed and limited, in that it cannot enable the data subject to identify the source of information. This right may be exercised only through the CNPD and in the presence of the President of the Press Council or his or her representative

2. Processing of personal data for scientific or historical research purposes, for statistical purposes, or for archiving purposes in the public interest

When personal data is processed for scientific or historical research purposes or for statistical purposes, the rights of the data subject specified under articles 15, 16, 18 and 21 GDPR may be limited provided that such rights would make impossible or seriously impede the accomplishment of the specific concerned purposes.

Such limitation on data subject rights may only be applied where the data controller puts in place an extensive set of additional appropriate safeguard measures for the rights and freedom of the data subject (Article 65 of the Law of August 1, 2018 on the organization of the National Data Protection Commission), such as, in particular:

- The appointment of a DPO
- Performing an impact assessment of the contemplated processing on the protection of personal data
- Anonymizing the data processed

In any event, the additional safeguard measures must be put in place in accordance with the nature, scope, context and purposes of the processing, as well as the risks for the rights and freedoms of the relevant data subjects. In this regard, if the data controller elects not to put in place one of the measures listed in Article 65 of the Law of August 1, 2018 on the organization of the National Data Protection Commission, it must then formally document and justify why it chose not to do so.

Finally, processing of special categories of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 9(2)(j), GDPR) is allowed under the same conditions (*ie,* putting in place additional appropriate safeguard measures as defined under Article 65 of the Law of August 1, 2018 on the organization of the National Data Protection Commission).

3. Processing of special categories of personal data

Genetic data may not be processed for purposes of exercising the controller's own rights in the field of employment and insurance law.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes, among others, binding corporate rules and standard contractual clauses. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. Explicit informed consent has been obtained
b. The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
d. The transfer is necessary for important reasons of public interest
e. The transfer is necessary for the establishment, exercise or defense of legal claims
f. The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
g. The transfer is made from a register, which according to EU or Member State law, is intended to provide information to the public, subject to certain conditions

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject. Notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State (transfers in response to such requests where there is no other legal basis for transfer will infringe the GDPR).

No specific provisions in the applicable local law.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However, the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

Article 65 of the Law of August 1, 2018 on the organization of the National Data Protection Commission provides specific technical measures that must be put in place for limited categories of processing (*ie,* processing of personal data for scientific or historical research purposes or for statistical purposes, and processing of special categories of personal data for archiving purposes in the public interest).

Such measures include:

- Resorting to an independent trusted third party for the anonymization or pseudonymization of the personal data
- Log files allowing for the identification of the purpose, date and time of consultation of the personal data as well as for the identification of the person having collected, modified or deleted the personal data

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

No specific provisions in the applicable local law.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent
- Data subjects’ rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data
- Certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.

- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The CNPD may:

- Impose administrative fines as provided for in Article 83 of the GDPR (however, it cannot impose such sanctions with respect to the State or municipalities)
- Impose on the controller or processor a penalty of up to five per cent (5%) of its average daily turnover in the previous financial year, respectively during the last financial year closed, as long as such controller or processor does not communicate an information requested by the CNPD pursuant to Article 58(1)(a) GDPR, or as long as such controller or processor does not abide by a corrective measure adopted by the CNPD pursuant to Article 58(2)(c)-(j) GDPR
- Impose sanctions (an imprisonment of 8 days or a fine of between EUR 251 and EUR 125,000) against anyone who knowingly prevents or hinders the performance of the CNPD's missions
- Order the insertion in full or by extracts of its decisions in newspapers or otherwise, at the expense of the person sanctioned

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing is permissible only in respect of subscribers who have given their prior consent.

Where a supplier obtains from its customers their electronic contact details for electronic mail, in the context of the sale of products or services, that supplier may use those electronic contact details for direct marketing of its own similar products or

services provided that customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message where the customer has not initially refused such use.

The transmission of unsolicited communications for purposes of direct marketing by means other than those referred to in the previous paragraphs shall be permissible only with the prior consent of the subscriber concerned.

No specific provisions in the applicable local law.

ONLINE PRIVACY

Traffic Data

For the purposes of the investigation, detection and prosecution of criminal offences, and solely with a view to enabling information to be made available, in so far as may be necessary, to the judicial authorities, any service provider or operator processing traffic data must retain such data for a period of six months. This obligation includes data related to the missed phone calls wherever these data are generated, stored or recorded. Beyond this period, the service provider or operator must erase such data unless made anonymous.

Traffic data may be processed for the purposes of marketing electronic communications services or providing value added services, to the extent and for the duration necessary for such supply or marketing of such services, provided that the provider of an electronic communications service or the operator has informed the subscriber or user concerned in advance of the types of traffic data processed and of the purpose and duration of the processing, and provided that the subscriber or user has given his or her consent, notwithstanding his or her right to object to such processing at any time.

Location Data other than Traffic Data

Service providers or operators have also the obligation to retain location data other than traffic data for a period of six months for the purposes of the investigation, detection and prosecution of criminal offences. This obligation includes data related to missed phone calls wherever these data are generated, stored or recorded. Beyond this period, the service provider or operator must erase such data unless made anonymous.

Service providers or operators may process location data other than traffic data relating to subscribers and users only if such data have been made anonymous or the subscriber or user concerned has given his or her consent, to the extent and for the duration necessary for the supply of a value added service.

Service providers and, where appropriate, operators shall inform subscribers or users in advance of the types of location data other than traffic data processed, of the purposes and duration of the processing and whether the data will be transmitted to third parties for the purpose of providing the value added service. Subscribers or users shall be given the possibility to withdraw their consent to the processing of location data other than traffic data at any time.

Where subscriber or user consent has been obtained for the processing of location data other than traffic data, the subscriber or user must continue to have the possibility, using a simple means free of charge, to temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication.

Cookies

Prior informed consent of a subscriber or user is required. The method of providing information and the right to refuse should be as user friendly as possible and, where it is technically possible and effective, the users consent may be expressed by appropriate browser or application settings.

The CNPD published official guidelines on cookies in October 2021.

KEY CONTACTS

Olivier Reisch
Partner
T +352 26 29 04 2017
olivier.reisch@dlapiper.com

David Alexandre
Counsel
T +352 26 29 04 2614
david.alexandre@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MACAU

Last modified 19 December 2023

LAW

Macau Personal Data Protection Law no. 8/2005 of August 22nd (Law).

DEFINITIONS

Definition of personal data

The Law defines personal data as any information of any type, in any format, including sound and image, related to a specific or identifiable natural person (data subject). An ‘identifiable natural person’ is anyone who can be identified, directly or indirectly, in particular by reference to a specific number or to one or more specific elements related to his or her physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

The Law defines sensitive personal data as any personal data revealing political persuasion or philosophical beliefs, political and joint trade union affiliation, religion, private life, racial or ethnical origin or data related to health or sex life, including genetic data.

NATIONAL DATA PROTECTION AUTHORITY

The Office for Personal Data Protection (OPDP) is the Macau regulatory authority responsible for supervising and coordinating the implementation of the Law.

REGISTRATION

The OPDP must be notified of any processing of personal data by a data controller, within 8 days from the commencement of the processing activity, unless an exemption applies.

For certain data categories (e.g. certain sensitive personal data, data regarding illicit activities or criminal and administrative offenses or credit and solvency data) and certain specific personal data processing, data controllers must obtain prior authorization from the OPDP.

The OPDP provides (official) forms that must be submitted regarding personal data processing, either in Portuguese or Chinese language, along with the following information (if applicable):

- Identification and contact details of the data controller and its representatives;
- The personal data processing purpose;
- Identification and contact details of any third party carrying out the personal data processing;
- The commencement date of the personal data processing;

- The categories of personal data processed (disclosing whether sensitive personal data, data concerning the suspicion of illicit activities, criminal and / or administrative offenses or data regarding credit and solvency are to be collected);
- The legal basis for processing personal data;
- The means and forms available to the data subject for updating his or her personal data;
- Any transfer of personal data outside Macau, along with the grounds for, and measures to be adopted with, the transfer;
- Personal data storage time limits;
- Interconnection of personal data with third parties; and
- Security measures adopted to protect the personal data.

DATA PROTECTION OFFICERS

There is no legal requirement to appoint a data protection officer in Macau.

COLLECTION & PROCESSING

Personal data may be processed only if the data subject has given his or her unequivocal consent or if processing is deemed necessary:

- Execution of an agreement where the data subject is a party, or, at the data subject’s request, negotiation in relation to such an agreement;
- Compliance with a legal obligation to which the data controller is subject;
- Protection of vital interests of the data subject if he or she is physically or legally unable to give his or her consent;
- Performance of a public interest assignment or exercise of public authority powers vested in the data controller or in a third party to whom the personal data is disclosed; or
- Pursuing a data controller's legitimate interest (or the legitimate interest of a third party to whom the data is disclosed), provided that the data subject’s interests or rights, liberties and guarantees do not prevail.

The data subject must be provided with all relevant processing information, including the identification of the data controller, the purpose of processing, and the means and forms available to the data subject for accessing, amending and deleting his or her personal data. Moreover, if applicable, the data subject should also be informed of the possibility of their data being transferred to a jurisdiction outside of Macau.

TRANSFER

The transfer of personal data outside Macau can only take place if the recipient country ensures an adequate level of personal data protection, unless the data subject has provided clear consent or the required legal conditions have been met, and the required filings have been made with the OPDP.

In view of the close relationship with Mainland China and the entry into force of the Chinese Personal Information Protection Law ("**PIPL**") with extraterritorial effect, the Macao Office for Personal Data Protection (OPDP) has urged local data controllers and processors to be aware of the data transfer requirements pursuant to the PIPL, including to proceed / take part in a data security assessment prior to the transfer of data from Mainland China to Macao.

SECURITY

The data controller must implement adequate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular, where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Such measures must ensure a security level appropriate to the risks represented by the personal data processing and the nature of the personal data, taking into consideration the state of the art and costs of the measures.

BREACH NOTIFICATION

The Law does not require data controllers to notify either the OPDP or data subjects about any personal data breach.

However, a new Law on Cybersecurity came into effect in 2019, which implemented the requirement to notify the Cybersecurity Incident Alert and Response Center (CARIC) and respective regulatory authority, in the event of a system breach – this obligation is, however, limited to operators of critical infrastructures.

ENFORCEMENT

Violations of the Law are subject to civil liability and administrative and criminal sanctions, including fines and / or imprisonment.

ELECTRONIC MARKETING

Under the Law, data subjects have the right to object, upon their request and free of charge, to the processing of their personal data for direct marketing purposes, to be informed before their personal data is disclosed or used by third parties for the purpose of direct marketing and to be expressly offered, also free of charge, the right to object to such disclosure or use.

ONLINE PRIVACY

The Law also applies in the online environment.

For example, a Macau company that collects personal data from Macau residents through its website (e.g. through cookies) must fulfil all obligations under the Law imposed on data processors. In particular, the Macau company must inform data subjects of the personal data processing purpose and notify the OPDP about the personal data processing.

KEY CONTACTS

MdME Lawyers
www.mdme.com.mo/en/

José Leitão
Partner
MdME
T +853 2833 3332
jose.leitao@mdme.com

Daniela Guerreiro
Associate
MdME
T +853 2833 3332
daniela.guerreiro@mdme.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MADAGASCAR

Last modified 1 December 2023

LAW

Law No. 2014-038 relating to protection of personal data is the main regulatory framework in Madagascar (the “**Data Protection Law**”).

After discussion at the National Assembly of Madagascar, the Data Protection Law was adopted on 16 December 2014. The Law was promulgated by the President of Republic of Madagascar on 9 January 2015 and published in the Official Gazette of the Republic of Madagascar on 09 June 2015.

The Data Protection Law has been in force for nine (09) years, but its application is not yet effective, as no implementing decree has been published.

DEFINITIONS

Definition of personal data

Personal data is any information relating to a natural person, whereby that person is or can be identified, directly or indirectly, by reference to a name, an identification number or to one or more elements specific to him / her such relating to physical, physiological, psychical, economic, cultural or social.

Definition of sensitive personal data

Sensitive personal data means data which includes information relating to:

- racial origin;
- biometric and genetic information;
- political opinion;
- religious belief or other convictions;
- trade-union affiliation; and / or
- health or sexual life.

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Law provides for the creation of the *Commission Malagasy sur l'Informatique et des Libertés* (“ CMIL”). However, the CMIL has not yet been established. The decree setting out the CMIL’s assignment and organisation has just been adopted by the Council of Government on 28 November 2023, and is awaiting adoption by the Council of Ministers. Its effective implementation is expected in 2024.

REGISTRATION

Except for certain data processing that is subject to exemption, authorisation, ministerial order or decree, the processing of personal data requires a prior declaration to the CMIL.

The prior declaration to the CMIL shall specify, where relevant, *inter alia*:

- the identity and the address of the data controller (*responsable du traitement*) (i.e. the natural or legal person who either alone or jointly with other persons determines the purpose and the means of the personal data processing and implements such processing itself or appoints a data processor for that purpose);
- the purpose(s) of the processing;
- the interconnections between databases;
- the types of personal data processed, their origins and the categories of persons affected by the processing;
- the duration for which the data will be kept;
- the department or persons in charge of implementing the data processing;
- the existence of data transfer to other country;
- the measures taken in order to ensure the security of the processing;
- the use of a data processor (*sous-traitant*).

The CMIL has to issue its decision on any authorisation application 2 months following receipt of the application. An additional time period of 2 months can be added to this period after decision of the President of the CMIL. The absence of decision of the CMIL during these periods is considered as a refusal of the application.

DATA PROTECTION OFFICERS

The Data Protection Law does require the appointment of a data protection officer (*délégué à la protection des données à caractère personnel*) in Madagascar provided that the CMIL is operational because the appointed data protection officer (“**DPO**”) should be notified to the CMIL.

The appointment of a DPO exempts an entity from making prior declarations to the CMIL.

The appointment of a DPO does not exempt an entity from requesting prior authorisation, where necessary (for example where there is a transfer of data to a country that does not provide an adequate level of protection for personal data).

The DPO must be a resident of Madagascar.

COLLECTION & PROCESSING

The following principles must be satisfied when personal data is collected and processed:

- all personal data must be processed fairly and lawfully for specific, explicit and legitimate purposes and subsequently processed in accordance with these purposes;
- all personal data collected must be adequate, relevant and non-excessive in view of the purposes for which it is collected;
- all personal data must be accurate and comprehensive and when necessary, kept up to date;
- all personal data must be retained no longer than is necessary for the purposes for which it is processed.

The processing of personal data must receive the data subject's prior consent or fulfill one of the following conditions:

- compliance with a legal obligation of the data controller;

- the purpose of the processing is to protect the individual's life;
- the purpose of the processing is to carry out a public service;
- the processing relates to the performance of a contract to which the concerned individual is a party, or pre-contractual measures requested by that individual;
- processing relates to the realisation of the legitimate interest of the data controller or the data recipient, subject to the interest and fundamental rights and liberties of the concerned individual.

The conditions for processing of sensitive personal data include most of the above conditions, but contain an additional list of more restrictive conditions that must also be satisfied such as requirement to obtain prior consent of the data subject, or in the absence of consent where the processing is undertaken to carry out a public service and is required by law or priorly authorised by the CMIL.

TRANSFER

The transfer of a data subject's personal data to a third party country is allowed only if the country guarantees to individuals a sufficient level of protection in terms of privacy and fundamental rights and liberties.

The sufficiency of the protection is assessed by considering all the circumstances surrounding the transfer, in particular the nature of the data, the purpose and the duration of the proposed processing, country of origin and country of final destination, rules of law, both general and sectorial in force in the country in question and any relevant codes of conduct or other rules and security measures which are complied with in that country.

Data controllers may transfer personal data to a third country that is not deemed to offer adequate protection only if:

- the data subject consents and duly informed of the absence of adequate protection;
- the transfer is necessary:
  - for the performance of a contract between the data controller and the individual, or pre-contractual measures;
  - undertaken at the individual's request;
  - for the conclusion or the performance of a contract in the interest of the individual, between the data controllers and a third party;
  - for the protection of the public interest;
  - for consultation of a public register intended for the public's information;
  - to comply with obligations allowing the acknowledgment, the exercise or the defense of a legal right.

In all cases, the data recipient in the third party country cannot transfer personal data to another country, except with the authorisation of the first data controller and the CMIL.

SECURITY

The data controller must take all useful precautions, with respect to the nature of the data and the risk presented by the processing, to preserve the security of the data and, amongst other things, prevent alteration, corruption or access by unauthorised third parties.

BREACH NOTIFICATION

The Data Protection Law does not set out any general or specific obligation to notify the CMIL or the data subject in the event of a data security breach.

ENFORCEMENT

The CMIL has the power to proceed with verifications of any data processing, and, as the case may be, to request a copy of every document that it considers useful in respect of verifications. The CMIL agents are authorised to carry out online inspections and on-site verifications of a data controller or a data processor.

In cases where the CMIL is of the opinion that a data controller or a data processor has contravened the provisions of the Data Protection Law, then it may serve, in accordance with the severity of the violation committed:

- warnings and notices to comply with the obligations defined in the Data Protection Law;
- notice of withdrawal of the authorisation;
- a financial sanction of up to 5% of the last financial year pre-tax turnover (not deducted from tax turnover).

The Data Protection Law provides that any processing of personal data in contravention with its provisions is considered an offence. For example, processing of personal data without prior declaration to or authorisation of the CMIL can result in imprisonment of 6 months to 2 years (Article 62 of the Data Protection Law).

In addition to any penalty, the Court may order the erasure of all or part of the personal data which was the object of the processing considered an offence.

ELECTRONIC MARKETING

The Data Protection Law does not provide specific restrictions on the use of electronic marketing. However, the data subject has a right to opt out of allowing their personal data to be used for marketing purposes without providing any reason.

ONLINE PRIVACY

The Data Protection Law does not yet address location data, cookies, local storage objects or other similar data-gathering tools.

KEY CONTACTS

Madagascar Law Offices

Sahondra Rabenarivo
Managing Partner
Madagascar Law Offices
T +(261) 20 23 25623
sahondra@aln-madagascar.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MALAYSIA

Last modified 21 December 2023

LAW

Malaysia's first comprehensive personal data protection legislation, the Personal Data Protection Act 2010 (PDPA), was passed by the Malaysian Parliament on June 2, 2010 and came into force on November 15, 2013.

As part of an ongoing review of the PDPA, the Personal Data Protection Commissioner of the Ministry of Communications and Multimedia Malaysia has issued Public Consultation Paper No. 01/2020 – Review of Personal Data Protection Act 2010 (PC01/2020) dated February 14, 2020 to seek the views and comments of the public on 22 issues set out in PC01/2020, some of which are set out below.

The Personal Data Protection Department (PDP Department) has indicated that, out of the 22 issues, 5 issues have been shortlisted as the key proposed amendments to the PDPA. In October 2023, the Deputy Minister of Communications, Teo Nie Ching, stated that the preparation of the bill to amend the PDPA is in the final stages, and she expected that the said bill will be tabled in March 2024.

DEFINITIONS

Definition of personal data

'Personal data' means any information in respect of commercial transactions that is:

- Being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
- Recorded with the intention that it should wholly or partly be processed by means of such equipment; or
- Recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, and, in each case.

...that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user.

Personal data includes any sensitive personal data or expression of opinion about the data subject. Personal data does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

Definition of sensitive personal data

'Sensitive personal data' means any personal data consisting of information as to the physical or mental health or condition of a data subject, his or her political opinions, his or her religious beliefs or other beliefs of a similar nature, the commission or alleged

commission by him or her of any offense or any other personal data as the Minister of Communications and Multimedia (Minister) may determine by published order. Other than the categories of sensitive personal data listed above, the Minister has not published any other types of personal data to be sensitive personal data as of December 15, 2020.

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to the PDPA, a Personal Data Protection Commissioner (Commissioner) has been appointed to implement the PDPA's provisions. The Commissioner will be advised by a Personal Data Protection Advisory Committee who will be appointed by the Minister, and will consist of one Chairman, three members from the public sector, and at least seven, but no more than eleven other members. The appointment of the Personal Data Protection Advisory Committee will not exceed a term of three years; however, members can be appointed for two successive terms.

The Commissioner's decisions can be appealed through the Personal Data Protection Appeal Tribunal. The following are examples of appealable decisions:

- Decisions relating to the registration of data users under Part II Division 2 of the PDPA;
- The refusal of the Commissioner to register a code of practice under Section 23(5) of the PDPA;
- The service of an enforcement notice under Section 108 of the PDPA;
- The refusal of the Commissioner to vary or cancel an enforcement notice under Section 109 of the PDPA; or
- The refusal of the Commissioner to conduct or continue an investigation that is based on a complaint under Part VIII of the PDPA.

If a data user is not satisfied with a decision of the Personal Data Protection Advisory Committee, the data user may proceed to file a judicial review of the decision in the Malaysian High Courts.

REGISTRATION

Currently, the PDPA requires the following classes of data users to register under the PDPA:

1. **Communications**
    - A licensee under the Communications and Multimedia Act 1998
    - A licensee under the Postal Services Act 2012
2. **Banking and financial institutions**
    - A licensed bank and licensed investment bank under the Financial Services Act 2013
    - A licensed Islamic bank and licensed international Islamic bank under the Islamic Financial Services Act 2013
    - A development financial institution under the Development Financial Institution Act 2002
3. **Insurance**
    - A licensed insurer under the Financial Services Act 2013
    - A licensed takaful operator under the Islamic Financial Services Act 2013
    - A licensed international takaful operator under the Islamic Financial Services Act 2013
4. **Health**
    - A licensee under the Private Healthcare Facilities and Services Act 1998
    - A holder of the certificate of registration of a private medical clinic or a private dental clinic under the Private Healthcare Facilities and Services Act 1998
    - A body corporate registered under the Registration of Pharmacists Act 1951
5. **Tourism and hospitalities**
    - A licensed person who carries on or operates a tourism training institution, licensed tour operator, licensed travel agent or licensed tourist guide under the Tourism Industry Act 1992
    - A person who carries on or operates a registered tourist accommodation premises under the Tourism Industry Act 1992
6. **Transportation**
    - Certain named transportations services providers
7. **Education**
    - A private higher educational institution registered under the Private Higher Educational Institutions Act 1996

- A private school or private educational institution registered under the Education Act 1996

8. **Direct selling**
    - A licensee under the Direct Sales and Anti-Pyramid Scheme Act 1993
9. **Services**
    - A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961 carrying on business as follows:
        - legal
        - audit
        - accountancy
        - engineering
        - architecture
    - A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961, who conducts retail dealing and wholesale dealing as defined under the Control Supplies Act 1961
    - A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961, who carries on the business of a private employment agency under the Private Employment Agencies Act 1981
10. **Real estate**
    - A licensed housing developer under the Housing Development (Control and Licensing) Act 1966
    - A licensed housing developer under the Housing Development (Control and Licensing) Enactment 1978, Sabah
    - A licensed housing developer under the Housing Developers (Control and Licensing) Ordinance 1993, Sarawak
11. **Utilities**
    - Certain named utilities services providers
12. **Pawnbroker**
    - A licensee under the Pawnbrokers Act 1972
13. **Moneylender**
    - A licensee under the Moneylenders Act 1951

Certificates of registration are valid for at least one year, after which data users must renew registrations and may not continue to process personal data.

Data users are also required to display their certificate of registration at a conspicuous place at their principal place of business, and a copy of the certificate at each branch, where applicable.

The Commissioner may designate a body as a data user forum for a class of data users. Data user forums can prepare codes of practice to govern compliance with the PDPA, which can be registered with the Commissioner. Once registered, all data users must comply with the provisions of the code, and non-compliance violates the PDPA. As of December 20, 2023, the Commissioner has published several codes of practice, including for the banking and financial sector, the aviation sector, the utilities sector, communications sector, the healthcare sector, and the insurance and takaful industry in Malaysia. There is also a general code of practice which applies to classes of data users required to be registered as data users under the PDPA who are currently not subject to any codes of practice registered by the Commissioner.

DATA PROTECTION OFFICERS

Currently, Malaysian law does not require that data users appoint a data protection officer.

However, pursuant to PC01/2020, the Commissioner is considering introducing an obligation in the PDPA for a data user to appoint a data protection officer and to introduce a guideline pertaining to such appointments.

The PDP Department has indicated that this requirement has been shortlisted as one of the five key proposed amendments to the PDPA which were under consideration (out of the 22 issues set out in P01/2020).

COLLECTION & PROCESSING

Under the PDPA, subject to certain exceptions, data users are generally required to obtain a data subject’s consent for the processing (which includes collection and disclosure) of his or her personal data. Where consent is required from a data subject under the age of eighteen, the data user must obtain consent from the parent, guardian or person who has parental responsibility for the data subject. The consent obtained from a data subject must be in a form that such consent can be recorded and maintained properly by the data user.

Pursuant to PC01/2020, the Commissioner has sought feedback on its proposal to amend the General Principle provision to add clarity to the data subject's consent, whether it should be in a specific provision and the impact of having a default consent.

Malaysian law contains additional data protection obligations, including, for example, a requirement to notify data subjects regarding the purpose for which their personal data are collected and a requirement to maintain a list of any personal data disclosures to third parties.

On December 23, 2015, the Commissioner published the Personal Data Protection Standard 2015 ("**Standards**"), which set out the Commission’s minimum requirements for processing personal data. The Standards include the following:

- Security Standard For Personal Data Processed Electronically
- Security Standard For Personal Data Processed Non-Electronically
- Retention Standard For Personal Data Processed Electronically And Non-Electronically
- Data Integrity Standard For Personal Data Processed Electronically And Non-Electronically

TRANSFER

Under the PDPA, a data user may not transfer personal data to jurisdictions outside of Malaysia unless that jurisdiction has been specified by the Minister. However, there are exceptions to this restriction, including the following:

- The data subject has given his or her consent to the transfer;
- The transfer is necessary for the performance of a contract between the data subject and the data user;
- The data user has taken all reasonable steps and exercised all due diligence to ensure that the personal data will not be processed in a manner that would contravene the PDPA; and
- The transfer is necessary to protect the data subject’s vital interests.

In 2017, the Commissioner published a draft Personal Data Protection (Transfer of Personal Data to Places Outside Malaysia) Order 2017 to obtain public feedback on the proposed jurisdictions to which personal data from Malaysia may be transferred. As of December 15, 2020, the Minister has yet to approve the safe harbor jurisdictions. Once approved, a data user may transfer personal data to these safe harbor jurisdictions without having to rely on the data subject's consent or other prescribed exceptions under the PDPA.

Pursuant to PC01/2020, the Commissioner acknowledged that a clear provision and the conditions for transferring personal data to places outside Malaysia are essential to facilitate e-commerce transactions and free trade agreements, and opined that a whitelist appears to curb and set a barrier for data users to transfer personal data to places outside Malaysia. In view of this, the Commissioner is considering restructuring the provision on cross border transfers under the PDPA and removing the whitelist provision. In this regard, the PDP Department has indicated that the whitelist regime will be replaced with a blacklist regime, where data users will generally be allowed to transfer personal data out of Malaysia (except to countries that have been blacklisted by the Minister).

In addition, the Commissioner also acknowledged that data users with overseas branches may need to exchange information with its branches at some point. The Commissioner is considering issuing a guideline on the mechanism and implementation of cross border data transfer and has sought feedback on the important matters to be considered in the proposed guideline.

SECURITY

Under the PDPA, data users have an obligation to take ‘practical’ steps to protect personal data, and in doing so, must develop and implement a security policy. The Commissioner may also, from time to time, set out security standards with which the data user must comply, and the data user is required to ensure that its data processors comply with these security standards.

In addition, the Standards provide separate security standards for personal data processed electronically and for personal data processed non-electronically (among others) and require data users to have regard to the Standards in taking practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

Pursuant to PC01/2020, the Commissioner observed that there are many new technologies such as facial recognition and smart trackers being used as data collection endpoints, and thus is considering issuing a policy regarding the endpoint security which uses technologies such as encryption. Additionally, it may be of interest to note that the PDP Department has indicated that the proposed amendment bill may impose a direct obligation on data processors to comply with the Security Principle under the PDPA.

BREACH NOTIFICATION

Currently, there is no requirement under the PDPA for data users to notify authorities regarding data breaches in Malaysia. Previously there was a voluntary data breach notification option available on the PDP Department’website, but the option appears to be no longer available. News reports dated October 5, 2018 suggest that Malaysia's laws could be updated, to include data breach notification requirements modeled after those under the European Union's General Data Protection Regulation (GDPR), including requiring providing notice to government authorities.

In addition, a news report dated March 20, 2019 reported that the Office of Personal Data Protection Malaysia's deputy commissioner, Rosmahyuddin Baharuddin, has also indicated that data breach notification is something that Malaysia is "seriously considering".

Notably, one of the issues for which feedback is sought in P01/2020 include reporting of data breaches. The points to be considered include, the proposed mandatory data breach notification, the impact of having all data users report about the data, and the elements to be considered in the guideline on data breach incident reporting. The PDP Department has indicated that data breach notification is shortlisted as one of the five key proposed amendments to the PDPA which is under consideration.

ENFORCEMENT

Under the PDPA, the Commissioner is empowered to implement and enforce the personal data protection laws and to monitor and supervise compliance with the provisions of the PDPA. Under the Personal Data Protection Regulations 2013, the Commissioner has the power to inspect the systems used in personal data processing and the data user is required, at all reasonable times, to make the systems available for inspection by the Commissioner or any inspection officer. The Commissioner or the inspection officers may require the production of the following during inspection:

- The record of the consent from a data subject maintained in respect of the processing of that data subject's personal data by the data user;
- The record of required written notices issued by the data user to the data subject;
- The list of personal data disclosures to third parties;
- The security policy developed and implemented by the data user;
- The record of compliance with data retention requirements;
- The record of compliance with data integrity requirements; and
- Such other related information which the Commissioner or any inspection officer deems necessary.

Violations of the PDPA and certain provisions of the Personal Data Protection Regulations 2013 are punishable with criminal liability. The prescribed penalties include fines, imprisonment or both. Directors, CEOs, managers or other similar officers will have joint and several liability for non-compliance by the body corporate, subject to a due diligence defense.

There is no express right under the PDPA allowing aggrieved data subjects to pursue a civil claim against data users for breaches of the PDPA.

However, under PCP 01/2020, the Commissioner has proposed to introduce a specific provision stating the right of a data subject to commence civil litigation against a data user.

ELECTRONIC MARKETING

The PDPA applies to electronic marketing activities that involve the processing of personal data for the purposes of commercial transactions. There are no specific provisions in the PDPA that deal with electronic marketing. However, the PDPA provides that a data subject may, at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances to cease or not to begin processing his or her personal data for direct marketing purposes. 'Direct marketing' means the communication by whatever means of any advertising or marketing material that is directed to particular individuals.

Pursuant to PCP 01/2020, the Commissioner is considering issuing a guideline to data users on the mechanism of digital and electronic marketing. The Commissioner has sought feedback on a proposed requirement on data users to provide a clear mechanism for data subjects to unsubscribe from online services and the elements to be considered in preparing the guideline on processing personal data in digital and electronic marketing.

The Commissioner is also considering issuing a guideline on the implementation of direct marketing for data users. Feedback from the public is sought as to whether a proposed data user is allowed to make the first direct marketing call to the data subject, the use of the 'opt-out' method, and the important elements to be considered in the preparation of such guideline.

ONLINE PRIVACY

There are no provisions in the PDPA that specifically address the issue of online privacy (including cookies and location data). However, any electronic processing of personal data in Malaysia will be subject to the PDPA and the Commissioner may issue further guidance on this issue in the future.

KEY CONTACTS

Skrine
www.skrine.com/

Jillian Chia
Partner
Skrine
T + 603 2081 3882
jc@skrine.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MALTA

Last modified 18 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The relevant law is the Data Protection Act 2018 (Act) (Chapter 586 of the Laws of Malta) and the Regulations (at present 9 in number) issued under it. The Act repealed and replaced the previous Data Protection Act (Chapter 440 of the Laws of Malta).

In 2020, Subsidiary Legislation 586.10 (‘Processing Of Data Concerning Health for Insurance Purposes Regulations’) was significantly amended. Pursuant to Article 9 of the GDPR, it was made explicit that processing of data concerning health shall be deemed to be in the substantial public interest when such processing is necessary for the purpose of the business of insurance or insurance distribution activities. However, this is made subject to suitable and specific measures designed to safeguard the fundamental rights and freedoms of data subjects.

The main legislative amendments that came into effect in 2021 were those to Subsidiary Legislation 586.07 (Processing of Personal Data (Education Sector) Regulations). The main purpose of these amendments was to bring the terminology used in these regulations in line with the wording of the GDPR rather than the previous local law. The full text, in English, is available here.

In 2021, certain procedural amendments were also made to the Act. The amending act (having the aim of providing for the amendment of various laws for the purpose of reforming the procedure for the making of various appointments) can be read here.

In 2023, a new Subsidiary Legislation was introduced: the Enforcement of the Rights of Data Subjects in Relation to Transfers of Personal Data to a Third Country or an International Organisation Regulations (S.L. 586.12). The scope and purpose of this law is to establish rights in Maltese law for third party beneficiaries with respect to transfers of personal data to a third country or an international organisation. This law provides a clear mechanism in Malta for data subjects to enforce their rights (including those granted under GDPR) when their personal data is transferred to a third country, even though they would not be parties to the instrument (either the Standard Contractual Clauses or any other appropriate safeguard), by virtue of which the third country transfer is being made. As a general principle of Maltese law, a contract is not normally deemed to have the power to confer rights to third parties, rendering S.L. 586.12 an exception to the rule, albeit, a necessary one. The full text of the law can be read here.

See all Maltese Legislation here.

DEFINITIONS

Personal data is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Data Protection Act reproduces the definitions provided by Article 4, GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single

establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Information and Data Protection Commissioner (Commissioner). Informally, the Office of the Information and Data Protection Commissioner (OIDPC).

Level 2, Airways House
Second Floor
High Street
Sliema SLM 1549
Malta

T: +356 2328 7100
F: +356 23287198

idpc.info@idpc.org.mt

www.idpc.org.mt

The Commissioner has the function (among others) of generally protecting individuals' data protection rights against privacy violations in personal data processing.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Under Article 7 of the Maltese DPA, data controllers must consult and gain prior authorization from the Commissioner to process in the public interest: genetic data, biometric data or data concerning health for statistical or research purposes or special categories of data relating to the management of social care services and systems.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale
- Its core activities consist of processing sensitive personal data on a large scale

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have expert knowledge (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Act does not derogate or further regulate from the provisions of the GDPR in this regard.

However, **DPOs must be notified to the Commissioner** (where Commissioner has jurisdiction) by sending, even via email, the following basic information:

- Data Controller identity
- name of DPO
- position
- mailing address
- email address
- contact number
- nature of business
- date of appointment, and
- whether the DPO is fulfilling this role for other data controllers.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous,*" and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services

- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to re-purpose personal data – *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract

- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision taking, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. Necessary for entering into or performing a contract
b. Authorized by EU or Member State law
c. The data subject has given their explicit (*ie,* opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The position under the Maltese Data Protection Act, 2018

The Act states that controllers and processors may derogate from the provisions of Articles 15, 16, 18 and 21 of the GDPR for the processing of personal data for scientific or historical research purposes or official statistics insofar as the exercise of the rights set out in those Articles:

1. Is likely to render impossible or seriously impair the achievement of those purposes, and
2. The data controller reasonably believes that such derogations are necessary for the fulfilment of those purposes.

Controllers and processors may also derogate from the obligations of Articles 15, 16, 18, 19, 20 and 21 of the GDPR for archiving purposes in the public interest. The same criteria ((1) and (2) above) must subsist for this derogation to apply.

Article 8 of the Act stipulates that an identity document shall only be processed when such processing is justified having regards to the purpose of processing and (1) the importance of a secure identification; or (2) any other valid reason as may be provided by law.

Personal data being processed for the purpose of exercising the right to freedom of expression and information, including processing for journalistic purposes or for the purpose of academic, artistic or literary expression, is exempt from compliance with the provisions of the GDPR (listed below), where, having regard to the right of freedom of expression and information in a democratic society, compliance with the following provisions would be incompatible with such processing purposes:

a. Chapter II (Principles)

- Article 5(1)(a) to (e) (principles relating to processing)
- Article 6 (lawfulness)
- Article 7 (conditions for consent)
- Article 10 (data relating to criminal convictions, etc.)
- Article 11(2) (processing not requiring identification)

b. Chapter III (rights of the data subject)

- Article 13(1) to (3) (personal data collected from data subject: information to be provided)
- Article 14(1) to (4) (personal data collected other than from the data subject)
- Article 15(1) to (3) (access to data and safeguards for third country transfers)
- Article 17(1) and (2) (right to erasure)
- Article 18(1)(a), (b) and (d) (restriction of processing)
- Article 20(1) and (2) (right to data portability)
- Article 21(1) (objections to processing)

c. Chapter IV (controller and processor)

- Article 25 (data protection by design and by default)
- Article 27 (representatives of controllers or processors not established in the Union)

- Article 30 (records of processing activities)
- Article 33 (notification of personal data breach to supervisory authority)
- Article 34 (communication of personal data breach to the data subject)
- Article 42 (certification)
- Article 43 (certification bodies)

d. Chapter VII (co-operation and consistency)

- Articles 60 to 62 (co-operation)
- Articles 63 to 67 (consistency)

Important note regarding age of consent: The processing of personal data of a child in relation to information society services has been lowered from eighteen (18) to thirteen (13) years of age by means of the ‘Processing of Children’s Personal Data in Relation to the Offer of Information Society Services Regulations’ (Subsidiary Legislation 586.11 issued under the Data Protection Act 2018). It is important to note that the age of consent for valid contract formation in Malta remains 18 years of age. This grey area is still subject to local authoritative interpretation. We are not aware of any such interpretations at time of writing.

Finally, in certain circumstances, the collection and processing of personal data are further regulated by local sector-specific regulations. By way of example, medical data relating to students can only be processed under specific conditions.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes, among others, binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. Explicit informed consent has been obtained
b. The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
d. The transfer is necessary for important reasons of public interest
e. The transfer is necessary for the establishment, exercise or defense of legal claims
f. The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
g. The transfer is made from a register, which according to EU or Member State law, is intended to provide information to the public, subject to certain conditions

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject. Notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State (transfers in response to such requests where there is no other legal basis for transfer will infringe the GDPR).

The Act does not derogate or further regulate from the provisions of the GDPR in this regard.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

The Act does not derogate or further regulate from the provisions of the GDPR in this regard.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The Act does not derogate or further regulate from the provisions of the GDPR in this regard.

The application form to be used when notifying data breaches to the OIDPC can be accessed here.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent
- Data subjects’ rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data
- Certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The position under the Maltese Data Protection Act, 2018

Appealing against a decision of the Commissioner

Any person against whom an administrative fine has been imposed by the Commissioner may appeal to the Data Protection Appeals Tribunal within 20 days from service of the Commissioner’s decision imposing such fine. An appeal to the Tribunal may be made on any of the following grounds:

- That a material error as to the facts has been made
- That there was a material procedural error
- That an error of law has been made
- That there was some material illegality, including unreasonableness or lack of proportionality

Within 2 days of filing an appeal, the Registry of the Tribunal shall:

- Serve a copy of the appeal on the Commissioner and request that he or she file a statement on the decision, together with any other information on which the decision was based within 20 days from the date on which the appeal was served
- Serve a copy of the appeal on the respondent(s) to the appealed decision, and request the respondent(s) file a reply within 20 days of service of the appeal

Appealing against a decision of the Data Protection Appeal Tribunal

Any party to an appeal before the Tribunal may appeal to the Court of Appeal by means of an application filed in the registry of that court within 20 days from the date on which the decision of the Tribunal was notified.

Fines against a public authority or body

The Commissioner may impose an administrative fine on a public authority or body of up to EUR 25,000 for each violation and an additional EUR 25 for each day during which such violation persists for an infringement under Article 83

(4) of the GDPR. The fine that the Commissioner may impose on a public authority or body for an infringement of Article 83(5) or (6) of the GDPR shall not exceed EUR 50,000 for each violation and additionally EUR 50 for each day during which such violation persists.

Any person who knowingly provides false information to the Commissioner when so requested or who does not comply with any lawful request pursuant to an investigation by the Commissioner, shall be guilty of an offence and upon conviction shall be liable to a fine (*multa*) of not less than EUR 1,250 and not more than EUR 50,000 or to imprisonment for six months.

Actions against a controller/processor

Without prejudice to any other available remedy, a person who believes that his or her rights under the GDPR or the Act have been infringed may file a sworn application in the First Hall Civil Court for an effective judicial remedy and in the same way may also institute an action for damages against the controller or processor who processes personal data in contravention of the provisions of the GDPR or this Act. If the court finds that the controller or processor is liable for damage caused pursuant to Article 82 of the GDPR, the court shall determine the amount of damages including, but not limited to, **moral damages**, due to the data subject.

Any action under Article 30 of this Act shall be instituted within 12 months from when the data subject became aware or should have reasonably become aware of such a contravention, whichever is earlier.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Act applies also to most electronic marketing activities since in the course of such activities, it is likely that ‘ personal data’ as defined above (including email) will be ‘processed’ as understood by the Act. In relation to direct marketing (even electronic), consent may be revoked at will by the data subject(s).

The controller is legally bound to inform the data subject that he or she may oppose such processing at no cost.

Apart from the Act, the ‘Processing of Personal Data (Electronic Communications Sector) Regulations’ (Subsidiary Legislation 586.01 issued under the Data Protection Act 2018) (the Electronic Communications Regulations) address a number of activities relating specifically to electronic marketing.

In the case of subscriber directories, the producer of such directories shall ensure (without charge to the subscriber) that before any personal data relating to the subscriber (who must be a natural person) is inserted in the directory, the subscriber is informed about the purposes of such a directory of subscribers and its intended uses (including information regarding search functions embedded in the electronic version of the directories). No personal data shall be included without the consent of the subscriber. In furnishing his consent the subscriber shall determine which data is to be included in the directory and is free to change, alter or withdraw such data at a later date. The personal data used in the directory must be limited to what is necessary to identify the subscriber and the number allocated to him, unless the subscriber has given additional consent authorizing the inclusion of additional personal data.

The Electronic Communications Regulations also deal with the issue of unsolicited communications. A person is prohibited from using any publicly available electronic communications service to engage in unsolicited communications for the purpose of direct marketing by means of:

- An automatic calling machine
- A facsimile machine
- Email

to a subscriber, irrespective of whether such subscriber is a natural person or a legal person, unless the subscriber has given his prior explicit consent in writing to the receipt of such a communication.

By way of exception to the above (informally known as the ‘soft opt-in’ rule), where a person has obtained from his customers their contact details for email in relation to the sale of a product or a service, in accordance with the Act that same person may use such details for direct marketing of its own similar products or services. However, the customers must be given the opportunity to object, free of charge and in an easy and simple manner, to such use of electronic contact details when they are collected and on the occasion of each message where the customer has not initially refused such use.

In all cases the practice of, inter alia, sending email for the purposes of direct marketing, disguising or concealing the identity of the sender or without providing a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

The Act does not change the position under the previous Data Protection Act (Chapter 440) and does not introduce derogations from the provisions of the GDPR in this regard. The proposed ePrivacy Regulation would need to be analyzed separately.

ONLINE PRIVACY

Cookie Compliance

Subsidiary Legislation 586.01, entitled ‘Processing of Personal Data (Electronic Communications Sector) Regulations' amended the regulations implementing Article 2(5) of Directive 2009/136/EC into Maltese Law.

The Commissioner has recently published a “**Guidance Note on Cookies Consent Requirements**” which can be read here.

Traffic Data

Under the Processing of Personal Data (Electronic Communications Sector) Regulations, traffic data relating to subscribers and users processed by an undertaking which provides publicly available electronic communications services or which provides a public communications network, must be erased or made anonymous when no longer required for the purpose of transmitting a communication.

Traffic data required for the purpose of subscriber billing or interconnection payments may be retained, provided however, that data retention is permissible only up to the period that a bill may lawfully be challenged or payment pursued.

Traffic data may be processed where the aim is to market or publicize the provision of a value-added service, however, the processing of such data shall only be permissible to the extent and for the duration necessary to render such services.

Processing of traffic data is also permissible by an undertaking providing publicly available electronic communication for the following purposes:

- Managing billing or traffic management
- Customer inquiries
- Fraud detection
- Rendering of value-added services

The Act does not introduce any new rules in this regard.

Location Data

Where location data (other than traffic data) relating to users or subscribers of public communications networks or of publicly available electronic communications services can be processed, such data may only be processed when it is made anonymous or with the consent of the users or subscribers, to the extent and for the duration necessary for the provision a value-added service.

Prior to obtaining user or subscriber consent, the undertaking providing the service shall inform them of the following:

- The type of location data which shall be processed
- The purpose and duration of processing
- Whether the processed data shall be transmitted to a third party for the purpose of providing the value-added service

A user or subscriber may withdraw consent for the processing of such location data (other than traffic data) at any time.

The Act does not change the previous position and does not derogate from the GDPR or further regulate in this regard.

KEY CONTACTS

Mamo TCV Advocates
www.mamotcv.com/

Dr. Claude Micallef-Grimaud
Partner
Mamo TCV Advocates
T +356 25 403 000
claude.micallefgrimaud@mamotcv.com

Dr. Warren Ciantar
Senior Associate
Mamo TCV Advocates
T +356 25 403 000
warren.ciantar@mamotcv.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MAURITIUS

Last modified 18 January 2024

LAW

Mauritius regulates data protection under the Data Protection Act 2017 (DPA 2017 or Act), proclaimed through Proclamation No. 3 of 2018 and effective on January 15, 2018. The Act repeals and replaces the Data Protection Act 2004, so as to align with the European Union General Data Protection Regulation 2016/679 (GDPR).

DEFINITIONS

Definition of personal data

Personal data is defined as any information relating to a data subject. A data subject is a natural person who is identified or identifiable, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Definition of sensitive personal data or special categories of personal data

Similar to the GDPR, the DPA 2017 refers to sensitive personal data as special categories of data. Special categories of data include personal data pertaining to any of the following about a data subject:

- Racial or ethnic origin
- Political opinion or adherence
- Religious or philosophical beliefs
- Membership of a trade union
- Physical or mental health or condition
- Sexual orientation, practices or preferences
- Genetic or biometric data that is uniquely identifying
- Commission or proceedings related to the commission of a criminal offense
- Such other personal data as the Commissioner may determine to be sensitive personal data

NATIONAL DATA PROTECTION AUTHORITY

Under DPA 2017, the Data Protection Office (DPO) is responsible for data protection oversight. The DPO is an independent and impartial public office that is not subject to the control or direction of any person or authority. The DPO is headed by the Data Protection Commissioner (Commissioner), with the assistance of public officers as may be necessary. The contact details of the DPO are:

Data Protection Office

5th Floor, SICOM Tower
Wall Street, Ebene
Republic of Mauritius

Telephone

+230 460 0251

Fax

+230 489 7341

Website

dataprotection.govmu.org/

Email

dpo@govmu.org

dpo2@govmu.org

REGISTRATION

Every person who intends to act as a data controller or a data processor (as defined below) must register with the Commissioner in a form approved by the Commissioner and is required to pay a prescribed registration fee. The Commissioner is authorized to approve applications and issue registration certificates, which are valid for three years.

Data processors and controllers must renew their registration within three months prior to the date that their registration expires. Failure to register or renew registration constitutes an offence under the Act, punishable by a fine not exceeding 200,000 or imprisonment for a term not to exceed five years.

A data controller is a person or public body who alone, or jointly with others, determines the purposes and means of personal data processing, and who has decision making power with respect to processing. A data processor is a person or public body who processes personal data on behalf of a controller.

Application for registration

Every registration application must include all of the following:

- Name and address
- Whether a representative has been nominated for the purposes of the Act, and the name and address of the representative
- A description of the personal data to be processed by the controller or processor, and of the category of data subjects, to which the personal data relate
- A statement as to whether data controller or processor holds, or is likely to hold, special categories of personal data
- A description of the purpose for which the personal data are to be processed
- A description of any recipient to whom the controller intends or may wish to disclose the personal data
- The name, or a description of, any country to which the proposed controller intends or may wish, directly or indirectly, to transfer, the data
- A general description of the risks, safeguards, security measures and mechanisms to ensure the protection of the personal data

A controller or processor who knowingly supplies false or misleading material information in their registration application commits an offense and could be held liable to a fine not to exceed 100,000 or imprisonment for a term not to exceed five years.

DATA PROTECTION OFFICERS

The DPA 2017 provides that every controller shall adopt policies and implement appropriate technical and organizational measures so as to ensure and be able to demonstrate that the processing of personal data is performed in accordance with the Act.

One of such measures is the mandatory requirement for the designation of a data protection officer (DPO) by all controllers and processors.

There can be one DPO for a group of companies, provided he is accessible for each company within the group.

The DPO can be an employee of the controller / processor, provided that there is no conflict of interest (if such position leads to the determination of purposes and means of processing) such as in the case of a chief executive, chief operating, chief financial, chief medical, head of marketing, head of human resource or head of IT.

The DPO can also be someone from outside the organisation.

The DPO needs to have professional experience and knowledge of data protection laws and standards.

The controller / processor is required to ensure that the DPO does not receive any instructions regarding the exercise of his functions-he should work in an independent environment and manner.

Role of DPO

The role of the DPO is to:

- advise the controller / processor and its employees about their obligations to comply with data protection laws and monitor compliance;
- train staff and conduct internal audits;
- advise on DPIAs;
- maintain a record of processing operations under his responsibility;
- be the first point of contact for the Data Protection Office and for individuals whose data are processed (employees, customers).

DPOs are not personally responsible for non-compliance with data protection requirements. Data protection compliance is the responsibility of the controller / processor.

COLLECTION & PROCESSING

Subject to exceptions provided under the Act, a controller cannot collect personal data unless the collection (a) is for a lawful purpose connected with a function or activity of the data controller, and (b) the collection is necessary for that purpose.

Where the data controller collects personal data directly from the data subject, the data controller shall at the time of collecting personal data ensure that the data subject concerned is informed of:

- The identity and contact details of the controller and, where applicable, its representative and any data protection officer
- The purpose for which the data are being collected
- The intended recipients of the data
- Whether or not the supply of the data by that data subject is voluntary or mandatory
- The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The existence of the right to request from the controller access to and rectification, restriction or erasure of personal data concerning the data subject or to object to the processing
- The existence of automated decision making, including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

- The period for which the personal data shall be stored
- The right to lodge a complaint with the Commissioner
- Where applicable, that the controller intends to transfer personal data to another country and on the level of suitable protection afforded by that country
- Any further information necessary to guarantee fair processing in respect of the data subject’s personal data, having regard to the specific circumstances in which the data are collected

Where data is not collected directly from the data subject concerned, the data controller or any person acting on his behalf shall ensure that the data subject is informed of the matters set out above.

There are six principles relating to the processing of personal data which are enumerated in the Act. Accordingly, every controller or processor need to ensure that personal data are:

- Processed lawfully, fairly and in a transparent manner in relation to any data subject
- Collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, and
- Processed in accordance with the rights of data subjects

For processing of data to be lawful, it must have a legal basis. One of the legal basis is consent. According to the DPA 2017, no person shall process personal data unless the data subject consents to the processing for one or more specified purposes. Consent is defined under the Act as any freely given, specific, informed and an unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmative action, by which he signifies his agreement to personal data relating to him being processed.

Processing shall also be lawful, when the processing is necessary for any of the following:

- The performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract
- Compliance with any legal obligation to which the controller is subject
- In order to protect the vital interests of the data subject or another person
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- The performance of any task carried out by a public authority
- The exercise, by any person in the public interest, of any other functions of a public nature
- The legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject
- The purpose of historical, statistical or scientific research

Special categories of personal data

Special categories of personal data, as defined above, cannot be processed unless the processing is based on one of the legal basis as described above and the processing is carried out in the course of the controller’s / processor’s legitimate activities with appropriate safeguards.

It is also possible to process special categories of personal data when:

- Processing relates to personal data which are manifestly made public by the data subject; or
- Processing is necessary for:
    - the establishment, exercise or defense of a legal claim;

- the purpose of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to a contract with a health professional subject to the obligation of professional secrecy;
- the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject; or
- protecting the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent.

TRANSFER

A controller or processor may transfer personal data to another country where any of the following apply:

- It has provided to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data; or
- The data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer owing to the absence of appropriate safeguards; or
- The transfer is necessary: (i) for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject’s request; (ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person; (iii) for reasons of public interest as provided by law; (iv) for the establishment, exercise or defense of a legal claim; or (v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or (vi) for the purpose of compelling legitimate interests pursued by the controller or the processor which are not overridden by the interests, rights and freedoms of the data subjects involved and where – (A) the transfer is not repetitive and concerns a limited number of data subjects; and (B) the controller or processor has assessed all the circumstances surrounding the data transfer operation and has, based on such assessment, provided to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data; or
- The transfer is made from a register which, according to law, is intended to provide information to the public and which is open for consultation by the public or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down by law for consultation are fulfilled in the particular case. Such transfer shall not involve the entirety of the personal data or entire categories of the personal data contained in the register and, where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or in case they are to be the recipients.

The Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the safeguards or the existence of compelling legitimate interests and may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as he may determine.

SECURITY

Under the DPA 2017, a controller or processor must, at the time of the determination of the means for processing and at the time of the processing, implement and maintain appropriate security and organizational measures for the prevention of unauthorized access to, alteration, disclosure or destruction of, or the accidental loss of the personal data.

Additionally, the controller or processor must ensure that measures provide a level of security appropriate to the harm that may result from the unauthorized access to, alteration, disclosure or destruction of, or the accidental loss of the personal data and the nature of the personal data concerned.

The measures referred to above shall include all of the following:

- The pseudonymization and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

In determining the appropriate security measures, in particular, where the processing involves the transmission of data over an information and communication network, a data controller shall have regard to the:

- State of technological development available
- Cost of implementing any of the security measures
- Special risks that exist in the processing of the data, and
- Nature of the data being processed

Where a controller is using the services of a processor – (a) the controller must choose a processor that is able to provide sufficient guarantees in respect of security and organizational measures for the purpose of complying with the security measures described above; and (b) the controller and the processor shall enter into a written contract which shall provide that – (i) the processor shall act only on instructions received from the controller; and (ii) the processor shall be bound by obligations of the controller as regards security measures to be taken.

If the purpose for keeping personal data has lapsed, the controller must destroy such data as soon as reasonably practicable and notify any data processor holding such data, who in turn must destroy the data specified by the controller as soon as is reasonably practicable.

Every controller or processor has to take all reasonable steps to ensure that any person employed by him or it is aware of, and complies with, the relevant security measures.

BREACH NOTIFICATION

Under the DPA 2017, a personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

A controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner. Where the Controller fails to notify the personal data breach within the 72 hours time limit, he should provide the Commissioner with the reasons for the delay. Where a processor becomes aware of a personal data breach, he shall notify the controller without undue delay.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the controller shall also communicate the personal data breach to the data subject without undue delay.

The communication of a personal data breach to the data subject shall not be required where:

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the breach, in particular, those that render the data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures to ensure that the high risk to the rights and freedoms of the data subject referred above is no longer likely to materialise; or
- it would involve disproportionate effort and the controller has made a public communication or similar measure whereby data subject is informed in an equally effective manner.

ENFORCEMENT

The DPA 2017 provides the Commissioner with enforcement authority. Where a complaint is made to the Commissioner that the Act or any regulations made under it, has or have been, is or are being, or is or are about to be, contravened, the Commissioner shall:

- investigate into the complaint or cause it to be investigated by an authorized officer, unless he is of the opinion that the complaint is frivolous or vexatious; and

- where he is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the complaint, notify, in writing, the individual who made the complaint of his decision in relation to it so that the individual may, where he considers that he is aggrieved by the decision, appeal against it to the Information and Communications Technologies (ICT) Appeal Tribunal.

If the Commissioner is of the opinion that a controller or a processor has contravened, is contravening or is about to contravene the DPA 2017, the Commissioner may serve an enforcement notice on the data controller or processor, requiring remedial efforts within a specified time frame.

A person who, without reasonable excuse, fails or refuses to comply with an enforcement notice commits an offense, and, on conviction, is liable to a fine not to exceed 50,000 Mauritian rupees and to imprisonment for a term not to exceed two years.

If the Commissioner has reasonable grounds to believe that data is vulnerable to loss or modification, she may make an application to a Judge in Chambers for an order for the expeditious preservation of such data.

The Commissioner may also carry out periodical audits of the systems and security measures of data controllers or data processors to ensure compliance with data protection principles laid down in the DPA 2017.

ELECTRONIC MARKETING

The Act regulates direct marketing, which is defined as the communication of any advertising or marketing material which is directed to any particular individual. The definition also encompasses electronic marketing.

The data subject may object to the processing of his or her personal data for purposes of direct marketing, including profiling to the extent relevant. Where a data subject objects to processing, his or her personal data may no longer be processed for that purpose. This right to object shall be explicitly brought to the attention of the data subject.

ONLINE PRIVACY

The Act applies to online privacy, though it does not contain specific provisions in relation to online privacy.

KEY CONTACTS

Juristconsult Chambers

Shalinee Dreepaul Halkhoree
Partner-Barrister
Juristconsult Chambers
T +230 465 00 20 Extension 225
sdreepaul@juristconsult.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MEXICO

Last modified 28 January 2024

LAW

The Federal Law on the Protection of Personal Data held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) ("the Law") entered into force on July 6, 2010.

Subsequently, the Executive Branch has also issued the following (collectively, with the Law, referred to herein as "Mexican Privacy Laws"):

- The Regulations to the Federal Law on the Protection of Personal Data held by Private Parties (Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares) (the Regulations), which entered into force on December 22, 2011
- The Privacy Notice Guidelines (the Guidelines), which entered into force on April 18, 2013
- The Recommendations on Personal Data Security, on November 30, 2013
- The Parameters for Self-Regulation regarding personal data, which entered into force on May 30, 2014
- The General Law for the Protection of Personal Data in Possession of Obligated Subjects (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados), which entered into force on January 27, 2017

On June 12, 2018, a decree was published in the Official Gazette of the Federation approving two important documents:

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data dated January 28, 1981, and its
- Additional Protocol regarding supervisory authorities and trans-border data flows dated November 8, 2001.

Mexican Privacy Laws apply to all personal data processing under any of the following circumstances:

- Processing carried out by a data controller established in Mexican territory
- Processing carried out by a data processor, regardless of its location, if the processing is performed on behalf of a data controller established in Mexico
- Processing by or on behalf of a data controller not located in Mexico, where Mexican legislation is applicable pursuant to the execution of an agreement or Mexico’s adherence to an international convention or
- Processing carried out within Mexican territory, on behalf of a data controller not established in Mexican territory, unless such processing is only for transit purposes

The Law only applies to private individuals or legal entities that process personal data, and not to the government, credit reporting companies governed by the Law Regulating Credit Reporting Companies or persons carrying out the collection and storage of personal data exclusively for personal use where it is not disclosed for commercial use. Further, Mexican Privacy Law also does not generally apply to business-to-business data, including:

- Data of legal entities.

- Data of individuals acting as merchants or professionals.
- Data of natural persons acting on behalf of a business (e.g., their employer), where the personal data processed is (a) limited to first and last names, title, position and functions performed, and business contact data, such as mailing or physical address, email address, telephone number and fax number, and (b) the personal data is processed solely for the purpose of representing the business or administering the business relationship (i.e., fulfilling orders, providing services, carrying out transactions between the business entities)

Additionally, the INAI has issued several documents and guidelines for the private sector regarding the processing of personal data, including the following:

- The Privacy Notice Guidelines (the Guidelines), which entered into force on April 18, 2013
- The Recommendations on Personal Data Security, on November 30, 2013
- The Parameters for Self-Regulation regarding personal data, which entered into force on May 30, 2014
- Recommendations for the Designation of the Data Protection Officer or the Data Protection Department
- Guideline to Implement Compensatory Measures
- Guideline for the orientation of the due processing of personal data in the activity of extrajudicial collection
- Guideline for the Secure Deletion of Personal Data
- Suggested minimum criteria for contracting cloud computing services that involve the processing of personal data
- Guideline for the Processing of Biometric Data.

DEFINITIONS

Definition of personal data

‘Personal data’ is any information concerning an identified or identifiable individual.

Definition of sensitive personal data

‘Sensitive personal data’ is personal data that affects the most intimate areas of the data subject’s life, which if misused, may lead to discrimination or entail a serious risk to the data subject. In particular, the definition includes data that may reveal any of the following:

- Racial or ethnic origin
- Past or present health conditions
- Genetic information
- Religious, philosophical or moral beliefs
- Union affiliation
- Political views
- Sexual orientation
- Pictures and videos
- Fingerprints
- Geolocation
- Banking information
- Signature

Other key definitions

'ARCO Rights' refer to the access, ratification, cancelation and opposition rights of data subjects, with respect to their personal data.

'Controller' or 'data controller' means the individual or private entity makes decisions regarding the processing of personal data.

'Data subject' means the individual to which the personal data belongs.

'Guidelines' means the guidelines issued by INAI, regarding the compliance with the principles and duties of the Data Privacy Law.

'INAI' refers to the National Institute of Transparency, Access to Information and Protection of Personal Data (***Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales***).

'Privacy notice' means the physical or electronic document, or document generated in any other form by the controller and made available to data subjects, prior to the processing of their personal data. There are three forms of a privacy notice: comprehensive or full-form, simplified, and short.

'Processing' means any collection, use, disclosure or storage of personal data made through any means, including any access, handling, exploitation, transfer or disposal of personal data.

'Processor' or 'data processor' means the individual or entity that separately or jointly with others processes personal data on behalf of the controller.

'Remittance' any communication of personal data carried out between the controller and the processor, within or outside Mexican territory.

'Third Party' means an individual or entity, whether national or foreigner, that is not the data subject, the controller or the processor of the personal data.

'Transfer' means any communication of personal data carried out between the controller and any third party.

NATIONAL DATA PROTECTION AUTHORITY

The National Institute of Transparency for Access to Information and Personal Data Protection (***Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales***) (INAI) and the Ministry of Economy (Secretaría de Economía) serve as Mexico’s data protection authorities.

REGISTRATION

Mexican law does not require registration with a data protection authority or other regulator in relation to the use of personal data.

DATA PROTECTION OFFICERS

All data controllers are required to designate a personal data officer or department (each, a Data Protection Officer) to handle requests from data subjects exercising their ARCO Rights (as defined in ‘Collection and Processing’) under the Law. Data Protection Officers are also responsible for overseeing and advising on the protection of personal data within their organizations.

COLLECTION & PROCESSING

Principles and obligations

In processing personal data, data controllers must observe the principles of legality, information, consent, notice, quality, purpose, loyalty, proportionality and accountability.

Pursuant to these principles:

- Personal data must be collected and processed fairly (and not through deceptive or fraudulent means) and lawfully
- Personal data must be collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes.
- Consent must be obtained, unless an exception applies.
- Processing of personal data must be adequate, relevant and not excessive in relation to the purposes for which it is collected. or further processed

- Personal data must be accurate and, if necessary, updated; every reasonable step must be taken to ensure that data that is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further processed, is erased or rectified., and
- Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed.
- Data subjects are entitled to a reasonable expectation of privacy in the processing of their personal data. In addition, personal data must be processed as agreed upon by the parties (in a privacy notice or otherwise) and in compliance with the Law.
- A privacy notice (Aviso de Privacidad) must be made available to data subjects prior to the processing of their personal data.

Required information for privacy notices

To legally process personal data, data controllers must provide a privacy notice (Aviso de Privacidad), which must be made available to a data subject prior to the processing of his or her personal data. The privacy notice may be provided to data subjects in printed, digital, visual or audio formats, or any other technology.

Controllers are required to notify data subjects of the main characteristics of the processing to which their personal data will be subject. This obligation is complied with through the privacy notice. Therefore, any data controller is required to prepare and make available to data subjects the relevant privacy notice(s) corresponding to their personal data. Controllers will have to make available distinct privacy notices for different categories of data subjects, such as personnel and customers.

The Guidelines permit the following three forms of privacy notice, depending on whether the personal data is obtained directly or indirectly from the data subject, and the context and space in which the personal data is collected:

- **Comprehensive privacy notice**: required to be provided when the personal data is obtained in-person from the data subject, for example, in a face-to-face interview.
- **Simplified privacy notice**: required to be provided when the data is obtained directly from the data subject, for example, when registering for an account on website or during a customer service call.
- **Short form privacy notice**: may be provided when the space for the privacy notice is limited and the Personal Data collected is minimum, for example, at an ATM, in a SMS, on a raffle ticket

Each of these forms must meet specific disclosure requirements, as described below, and the simplified and short-form notices must link to, or provide information about how to obtain, the comprehensive notice.

A **comprehensive privacy notice** must at least contain:

- The identity and address of the data controller
- A description of the personal data that will be processed
- Identification of any sensitive personal data that will be processed, and an affirmative statement that such data will be processed (if applicable)
- The purposes of the data processing, including the primary and any secondary purposes
- The options and means offered by the data controller to data subjects to limit the use, disclosure or processing of their data for any secondary purposes
- The means by which data subjects can revoke their consent
- The means for exercising rights of access, rectification, cancellation or objection (ARCO rights)
- Where appropriate, the types of data transfers to be made, including the purposes of such transfers and the identification of any third parties (not including processors) to whom personal data is transferred
- The procedure and means by which the data controller will notify the data subjects of changes to the Privacy Notice, and Identification of any sensitive personal data that will be processed

A **simplified privacy notice** must include, at least, the following information:

- The identity and address of the Controller
- The purposes of the data processing, including the primary and any secondary purposes

- The options and means offered by the data controller to data subjects to limit the use, disclosure or processing of their data for any secondary purposes
- How to access or obtain the comprehensive privacy notice

The **short form privacy notice** must include, at least, the following information:

- The identity and address of the Controller
- The purposes of the data processing, without distinguishing any secondary purposes
- The options and means offered by the data controller to data subjects to limit the use, disclosure or processing of their data for any secondary purposes

In addition to the required information, a privacy notice must be clear and in a comprehensible language, and with an easy structure and design, which means it should among other things, the privacy notice should not use inappropriate, ambiguous, or vague sentences, or refer to texts and documents that are not available for the data subject to review.

The data controller has the burden of proof to show that the privacy notice was provided to the data subjects prior to the processing of their personal data (unless an exception applies). However, controllers are not required to provide a privacy notice where:

- personal data is obtained indirectly and it is intended for historical, statistical, or scientific purposes
- where the personal data collected is not subject to Mexican Privacy Laws (*eg*, certain business-to-business data as described previously)

Consent to processing

Except as otherwise provided by the Law, some form of consent is required for all processing of personal data; depending upon the circumstances consent may be implicit, express, or express and written:

Implicit (or tacit) consent applies to the processing of personal data generally, except where the Law requires express or express written consent (or where consent is not required):

- Implicit consent is obtained where the data subject has been informed of the privacy notice and has not objected to or refused the processing of personal data as described in the privacy notice.
- Express consent (notice and opt-in) is required for o the processing of financial or asset data.
- Express consent may be obtained verbally, in writing, or via any technology or other unmistakable indication. Express and written consent is required for the processing of sensitive personal data. Express written consent may be obtained through the data subject’s written signature, electronic signature, or any other authentication mechanism.

In addition to the above, express or express written consent must be obtained where otherwise specifically required pursuant to an applicable law.

On the other hand, consent from the data subject is not required (but a privacy notice must still be made available) for the processing of personal data where any of the following apply:

- The processing is required pursuant to an applicable Mexican law
- The data is contained in publicly available sources
- The identity of the data subject has been disassociated from the data (*ie*, the data subject is no longer identifiable)
- Where the processing is for the purpose of fulfilling obligations pursuant to a legal relationship between the data subject and the data controller
- There is an emergency situation that could potentially harm an individual with regard to his or her person or property
- Processing is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the data subject is unable to give consent in the manner established by the General Health Law (Ley General de Salud) and other applicable laws, and said processing is carried out by a person subject to a duty of professional secrecy or an equivalent obligation, or
- Pursuant to a resolution issued by a competent authority

TRANSFER

Mexican privacy laws distinguish between 'transfers' of personal data (to third parties) and transmissions of personal data (to processors). Under Mexican Privacy Laws, a 'transfer' is any communication or transmission of personal data by or on behalf of the Controller to a third party (not including a processor). Where the data controller intends to transfer personal data to domestic or foreign third parties other than a data processor, it must provide the third parties with the privacy notice provided to the data subject and the purposes to which the data subject has limited the data processing. In addition, the controller must notify data subjects in the privacy notice of the transfer, including:

- that the transfer may be made, as well as to whom and for what purposes the personal data may be transferred.
- where consent to the transfer is required, that the data subject consents and how the data subject can refuse to consent to the relevant transfer(s).

The purpose of the transfer must be limited to the purpose and conditions informed in the privacy notice and consented to by the data subject (as applicable).

The third-party recipient must assume the same obligations as the data controller who has transferred the data.

Domestic and international transfers of personal data may be carried out without the consent of the data subject where the transfer is:

- Pursuant to a law or treaty to which Mexico is party
- Necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management
- Made to the holding company, subsidiaries or affiliates under the common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies as the data controller (provided they will comply with principles of Mexican Privacy Laws, the privacy notice provided to data subjects and the other applicable internal policies regarding data protection)
- Necessary by virtue of a contract executed or to be executed between the data controller and a third party in the interest of the data subject
- Necessary or legally required to safeguard public interest or for the administration of justice
- Necessary for the recognition, exercise or defense of a right in a judicial proceeding, or
- Necessary to maintain or comply with an obligation resulting from a legal relationship between the data controller and the data subject

The Regulations establish that communications or transmissions of personal data to processors do not need to be notified or consented to by the data subject. However, the data processor must do all of the following:

- Process personal data only according to the instructions of the data controller
- Not process personal data for a purpose other than as instructed by the data controller
- Implement the security measures required by the Law, the Regulations and other applicable laws and regulations
- Maintain the confidentiality of the personal data subject to processing
- Delete personal data that were processed after the legal relationship with the data controller ends or when instructed by the data controller, unless there is a legal requirement for the preservation of the personal data
- Not transfer personal data unless instructed by the data controller, the communication arises from subcontracting, or if so required by a competent authority

SECURITY

All data controllers must establish and maintain physical, technical and administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorized use, access or processing. They may not adopt security measures that are inferior to those they have in place to manage their own information.

The risk involved, potential consequences for the data subjects, sensitivity of the data and technological development must be taken into account when establishing security measures, and more care should be taken in the collection and process of sensitive personal data.

The Controller also has the obligation to train its personnel on the proper handling of personal data in order to ensure compliance with the Mexican Privacy Laws. Per the Guidelines, a controller must also establish, document and follow security policies and procedures, including:

- Maintaining an inventory of personal data and the relevant processing systems, and update this at least once per year with respect to sensitive personal data
- Identifying the duties and obligations of persons that processing personal data on behalf of the controller
- Conducting appropriate risk analyses to identify dangers and estimate risk of harm to personal data
- Establishing security measures applicable and confirm they are effectively implemented
- Assessing and improving security on an ongoing basis
- Establishing a roadmap to implement any missing security measures identified pursuant to a security breach (as necessary to prevent a recurrence of such breach)
- Performing reviews or audits of security program
- Maintaining records of the storage means for personal data

BREACH NOTIFICATION

Security breaches occurring at any stage of the processing that materially affect the property or moral rights of the data subject must be promptly reported by the data controller to the data subject.

Under Mexican Privacy Laws, a security breach of personal data includes any unauthorized:

- loss or destruction of personal data
- theft, loss or copying of personal data
- use, access or processing of personal data
- damage or alteration of personal data

If there is a breach of personal data, the controller must first analyze the causes of such breach; and then take steps to implement any corrective, preventive, improvement actions necessary to prevent the breach from recurring.

If a breach significantly affects the property or moral rights of the data subjects, the controller must immediately notify the affected data subjects, as soon as it confirms that the breach has occurred, so that the affected Data Subjects can take the corresponding measures.

The Regulations provide that breach notification must include at least the following information:

- The nature of the breach
- The personal data compromised
- Recommendations to the data subject concerning measures that he or she can adopt to protect his or her interests
- Immediate corrective actions implemented in response to the breach, and
- The means by which the data subject may obtain more information in regard to the data breach

ENFORCEMENT

Data subjects can enforce their ARCO Rights, when no response is obtained from the data controller via INAI and ultimately the court system.

If any breach of the Law or its Regulations is alleged, INAI may perform an on-site inspection at the data controller’s facilities to verify compliance with the Law.

Violations of the Law may result in monetary penalties or imprisonment, including the following:

INAI may impose monetary sanctions in the range of 100 to 320,000 times the Mexico City minimum wage (currently, MX $88.36, updated every year). Sanctions may be increased up to double the above amounts for violations involving sensitive personal data.

Three months to three years of imprisonment may be imposed on any person authorized to process personal data who, for profit, causes a security breach affecting the databases under its custody. Penalties will be doubled if sensitive personal data is involved.

Six months to five years of imprisonment may be imposed on any person who, with the aim of obtaining unlawful profit, processes personal data deceitfully, taking advantage of an error of the data subject or a person authorized to process such data. Penalties will be doubled if sensitive personal data is involved.

In determining the appropriate sanctions, the INAI will consider:

- The nature of the data
- The notorious inadmissibility of the refusal of the Data Controller, to carry out the acts requested by the data subject, in terms of this Law
- The intentional or unintentional nature of the action or omission constituting the offense
- The economic capacity of the data controller, and
- Recidivism

The sanctions imposed by the INAI are without prejudice to any further civil or criminal liability.

ELECTRONIC MARKETING

Email marketing constitutes personal data processing and is subject to the Law, including applicable notice and consent requirements.

ONLINE PRIVACY

The Regulations and Guidelines that address the use of cookies, web beacons and other analogous technologies, require that when a data controller uses online tracking mechanisms that permit the automatic collection of personal data, it provides prominent notice of the use of such technologies; the fact that personal data is being collected the type of personal data collected and the purpose of the collection and the options to disable such technologies.

An IP address alone may be considered personal data, however, there has not been a resolution or decision issued by the competent authority on this point.

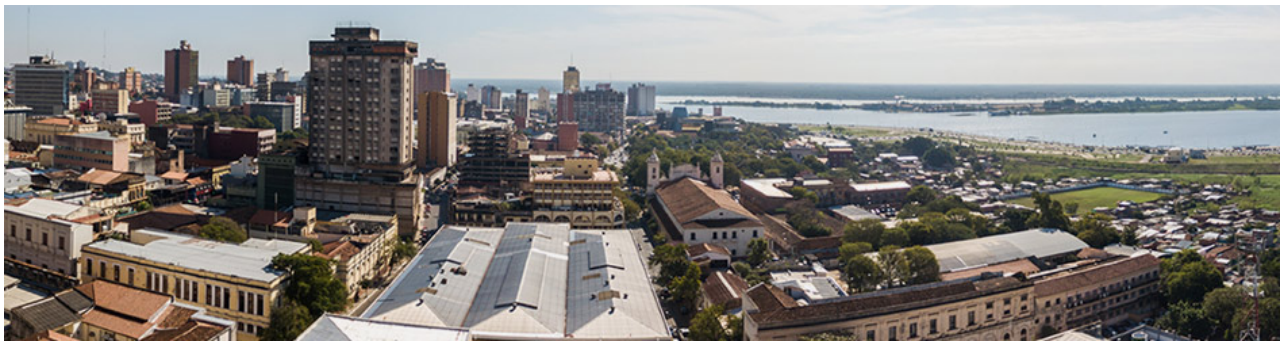
KEY CONTACTS

Gabriela Alaña
Partner
T + 52 55 5261.1817
gabriela.alana@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MOLDOVA



Last modified 18 January 2024

LAW

The main national legal acts regulating personal data protection in Moldova are:

- the Constitution of the Republic of Moldova (Article 28);
- the Law No. 133 of 08 July 2011 on Personal Data Protection;
- the Law No. 182 of 10 July 2008 regarding the approval of the National Centre for Personal Data Protection regulation, structure, staff-limit and its financial arrangements;
- the Government Decision No. 296 of 15 May 2012 on the approval of the Regulation regarding the Register of evidence of the personal data controllers;
- the Governmental Decision No. 1123 of 14 December 2010 on the approval of the requirements for the assurance of personal data security and their processing within the information systems of personal data.

The law on Personal Data Protection is the core legal act establishing the legal framework of personal data protection in Moldova. It has been adopted to harmonize the national regulations with the provisions of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

In the near future we expect the adoption of a new Law on Personal Data Protection which will transpose the provisions of the GDPR with some adjustments to Moldovan conditions.

Please note that Moldova is not an EU country and European provisions on personal data protection are not directly applicable in Moldova.

DEFINITIONS

Definition of personal data

Personal data is defined as “any information relating to an identified or identifiable natural person (“personal data subject”)”. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

Sensitive personal data is defined as special categories of personal data. Such special categories include data related to race, ethnic origin, political opinions, religious or philosophical beliefs, social belonging, data concerning health or sex life, as well as data relating to criminal convictions, administrative sanctions or coercive procedural measures.

NATIONAL DATA PROTECTION AUTHORITY

The National Centre for Personal Data Protection **(“NCPDP”)** is the national data protection authority. The permanent headquarters of the Centre are located in Chisinau, 48, Serghei Lazo str., MD-2004, T: +37322820801, F: +37322820807, www.datepersonale.md.

REGISTRATION

As of January 10, 2022, the requirement of mandatory registration or notification of personal data databases shall be abolished. However, according to the new provision, the controller shall consult with the NCPDP before starting any operations on processing of personal data in case if the data protection impact assessment indicates the processing would generate an increased risk.

The data protection impact assessment should contain at least the following information:

- The description of category of the data to be processed, the purpose of processing and legitimate interest (if any)
- The description of the necessity and proportionality of processing operations in relation to the purpose of processing
- Risk assessment for the rights and freedoms of data subjects, in particular, the source of those data, nature, specific degree of likelihood of materialization of the increased risk and the severity of that risk
- The description of risk prevention measures, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the provisions of the data protection law.

DATA PROTECTION OFFICERS

The appointment of an internal data protection officer is required, in the following cases:

- the processing is carried out by a public authority or institution, with the exception of courts acting in their judicial capacity;
- the main activities of the Data Controller or data processors consist of processing operations which, by virtue of their nature, their scope and / or their purposes, necessitate regular and systematic monitoring of data subjects on a large scale; and
- the main activities of the Data Controller or data processor consist of large-scale processing of special categories of data.

COLLECTION & PROCESSING

Personal data shall be processed with the consent of the personal data subject, unless an exception applies.

The consent of the data subjects is not necessary where the processing is necessary for:

- performance of a contract to which the personal data subject is party, in order to take steps at the request of the data subject prior to entering into a contract;
- carrying out an obligation of the controller, under the law;
- protection of the life, physical integrity or health of the personal data subject;
- performance of tasks carried out in the public interest or in the exercise of public authority prerogatives vested in the controller or in a third party to whom the personal data is disclosed;
- the purposes of legitimate interest pursued by the controller or by the third party to whom personal data is disclosed, except where such interest is overridden by the interests for fundamental rights and freedoms of the personal data subject;
- statistical, historical or scientific-research purposes, except where the personal data remains anonymous for a longer period of processing

Processing of special categories of personal data shall be prohibited, except for cases provided by the Law.

Personal data undergoing processing must be:

- processed fairly and lawfully;

- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits the identification of personal data subjects for no longer than is necessary for the purposes for which the data was collected and further processed.

The data controller shall ensure the confidentiality of personal data. The data controller and other persons who have access to the personal data, shall not disclose any information to a third party without the prior consent of the data subject unless one of the following exclusions applies:

- processing relates to data which is voluntary and manifestly made public by the personal data subject;
- the personal data is rendered anonymous.

The controller must implement appropriate technical and organizational measures to protect personal data against destruction, alteration, blocking, copying, disclosure, and against other unlawful forms of processing, that shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data.

TRANSFER

Transfers of personal data by a controller or a processor are permitted taking into account the principle of free movement of data to EU countries and to third countries that ensures an adequate level of protection of personal data subjects’ rights and of data intended for transfer.

The NCPDP is in charge of maintaining the list of the countries that ensures an adequate level of protection of personal data subject’s rights. The list of such jurisdictions has been elaborated by the NCPDCP. The list may be consulted, by accessing the following link.

The Law on Personal Data Protection also includes a list of context specific derogations, permitting transfers to countries that do not ensure an adequate level of protection:

- if the transfer is provided under an international treaty to which Moldova is a signatory;
- the data subject consents to the transfer;
- if the transfer is necessary for the conclusion or performance of an agreement or contract concluded between the personal data subject and the controller or between the controller and a third party in the interest of the personal data subject;
- if the transfer is necessary in order to protect the life, physical integrity or health of the personal data subject;
- if the transfer is carried out solely for journalistic, artistic, scientific and archive purposes of public interest;
- if the transfer is made to other companies from the same group as the data controller, provided that the mandatory corporate rules are observed;
- the transfer is necessary for the accomplishment of an important public interest, such as national defence, public order or national security, carrying out in good order a criminal trial or ascertaining, exercising or defending a right in court, on the condition that the personal data is processed solely in relation to this purpose and only for longer period is necessary to achieve it;
- if the processing takes place under the contract standard for cross-border data transmission, elaborated and approved by the NCPDCP, concluded by the data controller.

If only a data transfer agreement is to be concluded, our recommendation is to use as a template of data processing agreement the template approved by the NCPDCP. NCPDCP has elaborated the Standard Data Transfer Agreement, that may be used by the data controllers. Transferring data under this template elaborated by the NCPDCP shall be considered as an additional safeguard for the legitimacy of the transfer. The template Standard Data Transfer Agreement may be accessed here.

SECURITY

The controller must implement appropriate technical and organizational measures to protect personal data against destruction, alteration, blocking, copying, disclosure, and against other unlawful forms of processing, that shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data.

Governmental Decision No. 1123 of 14 December 2010 on the approval of the requirements for the assurance of personal data security and their processing within the information systems of personal data is used as a reference for the minimum-security measures to be implemented by the controller.

BREACH NOTIFICATION

Data controllers shall submit to the NCPDP an annual report on any security incidents involving information systems during that year.

ENFORCEMENT

The NCPDP is responsible for the enforcement of the Law on Personal Data Protection. The NCPDP is entitled to:

- carry out checks;
- consider complaints from data subjects;
- require the submission of necessary information about personal data processing by the data controller;
- require the undertaking of certain actions according to the law by the data processor, including discontinuance of the processing of personal data;
- file court actions;

Violation of personal data protection legislation may result in administrative liability. The maximum administrative penalty that can be imposed, as at the date of this review, is MDL (Moldovan lei) 15,000 which is about EUR 750.

If the violation has led to material or moral damages, the violator may be required by the court to reimburse such damages.

The NCPDP may also suspend or prohibit the processing of data if the rules on personal data protection are breached.

ELECTRONIC MARKETING

The Law regarding information society services dated July 22, 2004 provides for certain legal requirements for distribution of commercial electronic messages in the area of electronic commerce. In particular:

- commercial electronic messages are allowed only subject to the preliminary consent of a subscriber or addressee to receive such messages;
- the recipient shall have easy access to information regarding the individual or legal entity sending the message;
- commercial electronic messages regarding sales, promotional gifts, premiums etc. shall be unequivocally identified as such and the conditions for receiving of such promotions shall be clearly stated to avoid their ambiguous understanding.

ONLINE PRIVACY

At the date of this review, Moldovan law does not specifically regulate online privacy.

There are no specific requirements on data location, except for the requirement of the prior authorization of the cross-border transfer of data.

KEY CONTACTS

ACI Partners
www.aci.md

Marina Zanoga

Senior Associate
ACI Partners
T +373 22 279 323
mzanoga@aci.md

Nicolina Țurcan
Associate
ACI Partners
nturcan@aci.md

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MONACO

Last modified 18 January 2024

LAW

Within the Principality of Monaco (Monaco) data protection is regulated by Data Protection Law n° 1.165 of December 23, 1993, modified from time to time and notably by Law n° 1.353 of December 4, 2008 2018 (the “**DPL**”). Furthermore, Article 22 of the Monegasque Constitution protects the right to privacy and the secrecy of correspondence of every citizen.

Further, Monaco is part of the Council of Europe and entered into Convention n° 108 of the European Council of January 28, 1981 for the protection of individuals with regard to automatic processing of personal data, and into its protocol addendum regarding the controlling authorities and cross-border flows of data, both effective from April, 1st 2009 (through Sovereign Ordinances 2.118 and 2.119 of March 23, 2009).

Monaco is not part of the EU and did not adopt Data Protection Directive 95/46/EC (hereinafter referred to as the “ **European Directive**”) or its successor the General Data Protection Regulation (Regulation EU 2015/679) of April 27, 2016 (hereinafter referred to as the “**GDRP**”).

As a consequence, the European Commission does not consider Monaco as ensuring an adequate and sufficient level of protection in conformity to the Article 44 of the GDRP.

To address this issue, some of the European standards, and notably the European definition of “**personal data**”, have already been transposed into the DPL (which has implemented some of the European key concepts) and by other legislations dealing with the automated processing of personal data, in particular:

- Law n°1.482 of December 17, 2019, regarding the digital economy in general; and
- Law n°1.483 of December 17, 2019, regarding the creation of a digital identity (and thus, of a digital identification number) for citizens and residents of Monaco and, within this context, of a Monegasque National Register of Digital Identity.

A new draft law incorporating some of the European standards is also expected shortly.

It is also important to note that, pursuant to Article 3.2. of the GDPR, the GDPR is already applicable to companies established in Monaco that process personal data of persons (or “**data subjects**”) residing in the EU where such processing is related to:

i. the supply of goods or services to such persons (irrespective of a payment for such supply); and
ii. the monitoring of their behavior taking place within the Union.

It shall be noted that in such a case, the company established in Monaco may be required to designate in writing a representative in the European Union (article 27 of GDPR).

DEFINITIONS

Definition of personal data

Under the DPL, personal data is defined as data enabling identification of a determined or determinable person. Any individual who can be identified, directly or indirectly, notably by reference to an identification number or to one or more factors specific to their physical, psychological, psychological, economic, cultural, or social identity is deemed to be determinable.

Definition of sensitive personal data

While not expressly defined under the DPL, sensitive personal data is considered to be personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health / genetic data, sex life, data concerning morals or social matters.

Definition of data processing

Under the DPL, data processing is defined widely as any operation or set of operations performed on such data, whatever the process used (including collection, recording, organization, modification, storage, extraction, consultation, destruction, as well as exploitation, interconnection or reconciliation, transmission, broadcasting).

Definition of the data processor/controller

Under the DPL, the person in charge of the processing or “**Data controller**” shall be considered as any person (natural or legal entity governed by private or public law) who alone or jointly with others, determines the purpose and means of the processing and who decides of its implementation.

Definition of the data subject

Any person whose personal data are processed.

NATIONAL DATA PROTECTION AUTHORITY

The Monegasque regulator is the Commission for Control of Personal Data (*Commission de Contrôle des Informations Nominatives* or “**CCIN**”) whose composition was recently amended by Sovereign Ordinance n°8.575

The CCIN has different missions and powers, which mainly include (i) a mission of registration and examination of cases (e.g. it receives declarations of processing, expresses advices and opinions, issues authorizations when needed), (ii) a mission of council and proposal (e.g. it makes proposals to the competent authorities and recommendations, informs the data subjects of their rights and obligations, publishes reports) and (iii) a mission of control and investigation.

REGISTRATION

Data controllers, who process personal data must notify the CCIN and request approval so that their processing of personal data may be registered. Any changes to the processing of personal data will require the registration to be amended. Concerning data controllers who are legal persons governed by public law, public authorities and bodies governed by private law with a mission of general interest, the decision shall be taken by the competent authorities or bodies following a reasoned opinion from the CCIN. A recent Ministerial Order of 18 March 2021 has brought some changes to this procedure.

Any natural or legal entities governed by private law who intend to implement automated data processing including personal information must first complete the required procedure with the CCIN.

There are four possible procedures to follow:

- Ordinary declaration (all nature or legal persons governed by private law usually fall under the ordinary declaration procedure);

- Simplified declaration (all processing compliant to a referenced Ministerial Order and only when it is clearly established that the processing operations do not adversely affect the rights and freedoms of the data subjects);

- Authorization request (only for automated processing of personal data relating to suspected unlawful activities, offences or security measures or including biometric data required to check persons’ identities, or for the purpose of surveillance);

- Legal advisory request (only processing relating to research in the field of health - excluding biomedical research and for processing implemented by natural or legal persons governed by public law, public authorities, organizations governed by private law entrusted with a mission of general interest or a concessionaire of public utility).

The data controller must decide which procedure is the most adapted to the processing he wants to implement. To do so, he needs to analyze the purpose of the processing, and depending on this purpose, complete one of the aforementioned procedures (ordinary request, simplified request, authorization request, or legal advisory request).

The notification to the CCIN should include at least the following information:

- What data is being collected

- Why the data will be processed

- The categories of data subject

- Whether the data will be transferred either within or outside the Monaco.

DATA PROTECTION OFFICERS

There is no requirement in Monaco for organizations to appoint a data protection officer.

However, appointing a data protection officer is viewed by the CCIN as evidence of a company’s measure taken in order to ensure compliance with the data protection legislation. In practice however, companies in Monaco do not generally appoint data protection officers.

When appointed in these companies, he is usually responsible for informing and advising the members of the entity on the legal obligations regarding data processing and for cooperating with the CCIN.

COLLECTION & PROCESSING

Data processing must be justified by at least one of the following bases:

- The data subject’s consent

- A legal duty imposed to the data controller

- A public purpose

- The performance of a contract entered into between the data controller and the data subject

- The data controller’s legitimate interests, unless the data subject’s fundamental rights and liberties outweigh the controller’s legitimate interests

If sensitive personal data is processed, at least one of the above bases must be met plus one from an additional list of more stringent conditions (determined in Article 12 of DPL).

Additionally, the data controller must provide the data subject with fair processing information. This includes information about the identity of the data controller, the purposes of processing, the identity of recipients, the right to oppose, access and amend their data and any other information needed under the circumstances to ensure that the processing is fair.

TRANSFER

Monaco is not part of the EU, so the DPL does not distinguish between EEA jurisdictions and non-EEA jurisdictions.

However, the DPL provides that the transfer of data is authorized for cross-border access, storage and processing of data only to a country which offers equivalent data protection and reciprocity (and in particular circumstances, including for example when the data subjects gave his consent for such transfer or when the transfer of data is necessary to save his life or a public interest).

The CCIN has established a list of the countries deemed to offer equivalent protection and reciprocity.

Data transfers to countries with an adequate level of protection are not subject to the authorization by the CCIN.

The CCIN has adopted a position of principle and decided that all personal data transfers to a country or an organization which does not ensure an adequate level of protection should, in any event, be submitted to the Commission in the form of a transfer authorization application. Subsequently, the CCIN affirmed that it is necessary to submit a transfer authorization application to the Commission if personal data will be accessed from a country that does not have an adequate level of protection.

GDPR has an impact on data transfers to and from Monaco. Two situations must be distinguished:

- Companies of the European Union that want to send data to Monaco:

  They should no longer have to carry out any specific formalities with their supervisory authority as long as tools to protect the data are put in place between the European data controller and his subcontractor or subsidiary, notably:

  - An approved code of conduct pursuant to Article 40 of the GDPR;
  - An approved certification mechanism pursuant to Article 42 of the GDPR.
  - Standard data protection clauses approved by the European Commission (art.46);
  - Binding corporate rules (art.47);

- Companies that want to send data from Monaco

As described above, they are still subject to the data transfer formalities of the CCIN if they wish to send data to a country which does not have an adequate level of protection.

SECURITY

Data controllers must take appropriate technical and organizational measures designed to protect against unauthorized or unlawful processing, accidental loss or destruction of, or damage to, personal data.

Measures implemented must ensure an adequate level of security with regard to the risks posed by processing and by the nature of the data to be protected.

Where the data controller or their representative engages a service provider to process personal data, they must ensure that the service provider is able to comply with the obligations laid down in the two previous paragraphs.

The implementation of processing by such service provider must be governed by a written agreement between the subcontractor and the data controller that stipulates specifically that the service provider and his employees work under the sole directive of the data controller, and that he is also accountable for the obligations relating to the security of the processing.

BREACH NOTIFICATION

There is no mandatory requirement in the DPL to report security breaches or losses to the CCIN or to data subjects.

ENFORCEMENT

The CCIN and Monegasque Courts are responsible for enforcing the DPL. If the CCIN becomes aware that a data controller is in breach of the DPL, it can serve an enforcement notice requiring the data controller to resolve the non-compliance. Failure to comply with an enforcement notice is a criminal offense and can be punished on conviction with imprisonment of one month to one year or a fine of between €9,000 and €90,000 or both.

Sanctions remain rare. The CCIN website only mentions one decision of sanction dated July 18, 2017, which was a warning and the fixation of an action plan to implement corrective measures, against a Monegasque company which didn’t submit to the CCIN a request to conduct automated processing of personal data.

ELECTRONIC MARKETING

Prior to implementing any electronic marketing activity the CCIN must be notified, as electronic marketing activities may use personal data. The DPL does not prohibit the use of personal data for the purpose of electronic marketing *per se*. However, when implementing electronic marketing activities a company must respect the provisions of Articles 1, 10-1, 10-2 and 14 of the DPL.

The automated or non-automated processing of personal data must not infringe the fundamental rights and freedoms enshrined in Title III of the Constitution.

When marketing, personal data must be:

- Collected and processed fairly and lawfully
- Collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes
- Adequate, relevant and not excessive in relation to the purposes for which it is collected and / or further processed
- Accurate and, if necessary, updated; every reasonable step must be taken to ensure that data which is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further processed, is erased or rectified
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed.

Processing of personal data must be justified by one of the following bases:

- By consent from the data subject(s)
- By compliance with a legal obligation to which the data controller or their representative is subject
- By it being in the public interest
- By the performance of a contract or pre-contractual measures with the data subject
- By the fulfillment of a legitimate motive on the part of the data controller or their representative or by the recipient, on condition that the interests or fundamental rights and freedoms of the data subject are not infringed

Data subjects from whom personal data is collected must be informed of all of the following:

- The data controller’s identity and, if applicable, the identity of their representative in Monaco

- The purpose of processing
- The obligatory or optional nature of replies
- The consequences for data subjects of failure to reply
- The identity of recipients or categories of recipients
- Their right to oppose, access and rectify their data
- Their right to oppose disclosure to and use of personal data by a third party, or the disclosure for the purposes of the third party’s commercial use, including marketing

ONLINE PRIVACY

Prior to the use of traffic data, location data and cookies the CCIN must be notified. The use of traffic data, location data and cookies will have to comply with the provisions of the DPL.

In its Deliberation No. 2019-083 of May 15, 2019, the CCIN has specified the main principles applicable to the methods of depositing cookies and other tracers on the terminals of network users.

In this recommendation the CCIN insists on the requirement to insert a banner appearing as soon as an Internet user arrives on the visited site. It is also requested that no cookie other than those necessary for the operation be deposited in the user's terminal without its consent.

The banner must not be solely for information purposes but must allow the approval or deactivation of the deposit of cookies directly on the site by a positive action of the user.

According to the CCIN, the employer cannot access the contents of private messages sent or received from the professional e-mail system without the employee presence and agreement.

However, in order for messages to be considered private, it is necessary for employees to identify them as such for example by specifying in the message's subject key words such as "private", or "personal".

KEY CONTACTS

Gordon S. Blair Law Offices
gordonblair.com/

Gilbert Delacour
CEO
Gordon S. Blair Law Offices
T +377 93 25 84 00
gilbertdelacour@gordonblair.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MONGOLIA

Last modified 25 December 2023

LAW

On 17 December 2021, the Parliament of Mongolia (the “**Parliament**”) adopted the Law of Mongolia on Personal Data Protection (the “**Data Protection Law**”) which came into effect and full force from 1 May 2022. The Data Protection Law applies to matters related to personal privacy and relations in connection with the collecting, processing, using, and security of Personal Data (as defined below) of an individual, as well as the collection, processing and use of individual’s Personal Data with the help of technology and software. The Data Protection Law regulates the handling of Personal Data and Sensitive Personal Data by Data Controllers (as defined below).

The Data Protection Law defines specific components of Personal Data and persons that are subject to regulations of the Data Protection Law. For instance, “data owner” means any individual (or his / her legal representative) who can be determined by his / her Personal Data defined under the Data Protection Law (“**Data Owner**”) and “data controller” means a natural or legal person, who collects, processes and uses Personal Data based on the permission of the Data Owner or in accordance with the law (“**Data Controller**”).

The Data Protection Law mainly divides human data (information) into two categories:

- Personal Data; and
- Sensitive Personal Data.

DEFINITIONS

Definition of personal data

Pursuant to Article 4.1.11 of the Data Protection Law, the following information refers to Personal Data:

- sensitive personal data;
- first and last name;
- date and place of birth;
- permanent address and location data;
- citizen’s registration number;
- properties;
- education and membership;
- online identifiers; and
- any other information that can be used to directly or indirectly identify a natural person.

Definition of sensitive personal data

Pursuant to the Data Protection Law, Sensitive Personal Data is subject to personal privacy. Sensitive Personal Data as defined in Article 4.1.12 of the Data Protection Law means:

- ethnicity and race;
- religion and beliefs;
- health, correspondence, genetic and biometric data;
- personal key of an electronic signature;
- criminal status and record; and
- any data concerning sexual orientation and sexual relationships.

NATIONAL DATA PROTECTION AUTHORITY

The National Human Rights Commission, the Ministry of Digital Development and Communications, and other relevant state authorities have various degrees of oversight of data protection under Chapter 6 of the Data Protection Law.

The Human Rights Commission is entitled to exercise the following with respect to data protection:

- monitor the implementation of the legislation on protection of Personal Data, organise public awareness and advocacy activities and submit requirements and recommendations to relevant organisations and provide comment on the relevant regulations;
- receive complaints and information for investigation or initiate an investigation in its sole discretion if it is considered that human rights and freedoms protected under the Data Protection Law have been infringed or potentially infringed in the course of collecting, processing, using and protecting Personal Data and submit requirements and recommendations to the relevant organisations;
- provide requirement and recommendations to the relevant entities in the context of collecting, processing, using and protecting Sensitive Personal Data;
- receive and review records submitted by Data Controllers regarding the violations detected during the collection, processing and use of Personal Data and the measures taken to eliminate its negative consequences, and make recommendations on further issues to be considered; and
- make recommendations for the prevention of violations of human rights and freedoms in the collection, processing and use of information through technology without human intervention.

The Ministry of Digital Development and Communications is entitled to exercise the following with respect to data protection:

- maintain the implementation of legislation on protection of Personal Data, organise public awareness and advocacy activities, provide professional advice and cooperate with the relevant organisations;
- adopt the technological safety requirement and regulations to be followed in the processing of personal sensitive, genetics and biometric data; and
- receive and register information about security breaches and cyber-attacks on information systems intended for data collection, processing and use, and take necessary measures immediately.

In addition, other state authorities are entitled to monitor the collection, processing and use of Personal Data by Data Controllers within the scope of their functions specified under relevant laws.

REGISTRATION

There is no registration requirement for Data Controllers or data processing activities except that Data Controllers have the obligation to keep records of:

- its activities of collection, processing and use of Personal Data; and
- its response to damages occurred to Personal Data.

Data Controllers are required to submit records of their response to damages occurred to Personal Data to the National Human Rights Commission annually or at any time as requested by the National Human Rights Commission.

DATA PROTECTION OFFICERS

Data Controllers must have a unit or personnel in charge with the information and data security. The Data Protection Law provides that Data Controllers and any person who processes the data must adopt internal rules and regulations on:

- maintenance of information security; and
- measures to be taken in case of data loss and a plan to deliver information to the Data Owner and the relevant state authority.

In this regard, organisations, as a Data Controller and processor, may appoint a data protection officer of their own volition.

COLLECTION & PROCESSING

In accordance with Chapter 2 of the Data Protection Law, state authorities, individuals, legal entities and other natural persons may collect, process and use (i) Personal Data and (ii) Sensitive Personal Data on the grounds provided by law and with the permission of the Data Owner.

The Data Protection Law mainly divides the collection and processing of Personal and Sensitive Personal Data as follows:

- collection and processing of Personal Data;
- collection and processing of Sensitive Personal Data;
- collection and processing of Genetics and Biometric data (types of Sensitive Personal Data); and
- collection and processing of Personal Data after death of the Data Owner.

State authorities can collect and process Personal Data if:

- permitted to by the Data Owner or permitted by law;
- execution and enforcement of contractual obligations;
- exercising the rights and obligations by the Data Controller during the employment relations;
- enforcement of obligations under the international treaties to which Mongolia is a party to; or
- enforcement actions by authorities as provided under applicable laws without interfering with the legitimate interests and rights of the Data Owner.

Legal entity and any persons other than the state authority can collect and process Personal Data if:

- permitted by the Data Owner or permitted by law;
- execution and enforcement of contractual obligations;
- exercising the rights and obligations by the Data Controller during the employment relations;
- Personal Data became legally available to the public; or
- making historical, scientific, artistic and literary works by maintaining the anonymity of the Data Owner.

Unless otherwise provided under relevant laws, the Data Controller must obtain digital / electronic or written permission from the Data Owner upon presenting the following terms and conditions to the Data Owner:

- definitive purpose of collecting, processing and using the Personal Data;
- name and contact information of the Data Controller;
- list of Personal Data to be collected, processed, and used;
- period of processing and using Personal Data;
- whether to make the Personal Data publicly available;
- whether to transfer Personal Data to other persons together with the name of recipient and list of Personal Data to be transferred; and
- form of cancelling the permission.

The collection, processing and use of Sensitive Personal Data is prohibited except as follows:

- state authorities and other persons as permitted by the Data Owner;

- health worker to exercise their rights and responsibilities under applicable laws in order to protect the health of an individual; or
- in the process of providing explanations, declarations and evidence in accordance with the law on claims of citizens or legal entities.

Genetic and Biometric data can only be collected and used by the following state authorities in accordance with applicable laws:

- non-overlapping data of the human body (fingerprints) by the state registration authority for the purposes of civil registration and overseeing the voter registration;
- biometric data by the border protection authority for the purpose of identifying and verifying a foreign citizen crossing the state border;
- genetic and biometric information by the competent authorities specified in the law for the purpose of combating, preventing and investigating crimes and violations;
- genetic and biometric data by court forensic organisation for forensic examination of criminal, civil, administrative and other cases and dispute proceedings;
- biometric information of the Parliament member for the purposes of attendance and voting; and an employer may, with the employee's permission, use biometric data other than non-identifiable human data (fingerprints) to facilitate the identification and verification of employees in accordance with the internal employment regulations established in accordance with the Labour Law.

Also, Personal Data and Sensitive Personal Data may be collected, processed and used for (i) journalistic purposes or (ii) for the purpose of creating historical, scientific, artistic and literary works and preparing statistical information based on the permission from the Data Owner.

In addition, the Data Protection Law provides that unless otherwise provided by law, (i) if the Data Owner has died or is considered dead, the relevant data shall be collected, processed and used with the written permission of the successor, his / her family member or legal representative and (ii) permission to collect, process or use Sensitive Personal Data is not required 70 years after the death of the Data Owner.

TRANSFER

Under the Data Protection Law, transfer of Personal Data is prohibited unless otherwise approved under the relevant laws or permitted by the Data Owner.

SECURITY

Data Controllers must take the following measures for the purpose of maintaining data security:

- adopt internal data security rules and regulations;
- approve a plan in accordance with the law to take measures and deliver notice to the state authority and the Data Owner in the event of data loss;
- take all measures to ensure the integrity, confidentiality and accessibility of information technology system used for data collection, processing and use;
- adopt and follow procedures and instructions on restricting the use of data, deleting the data and making it impossible to identify the Data Owner; and
- in the event of making decisions that affect the rights, freedom and legitimate interests of the Data Owner or regularly processing Sensitive Personal Data, the Data Controller must evaluate the situation in order to ensure the security of data processing activities. Guidelines and procedures for the evaluation will be adopted by the Ministry of Digital Development and Communications as recommended by the National Human Rights Commission.

On 11 September 2023, the Ministry of Digital Development and Communications adopted the procedure on "General requirement for maintaining information security during the collection, processing and use of Personal Data" ("**Information Security Requirement**"). As per the Information Security Requirement, the Data Controller must follow

the below principles when collecting, processing and using the Sensitive Personal Data in addition to those provided under the Data Protection Law:

- transparency;
- fit for purpose;
- maintain storage limitations;
- responsible;
- based on risk evaluation; and
- have integrated information system.

According to the Information Security Requirement, the Data Controller must comply with certain technological security requirements, including:

- adopt and implement internal information security regulation;
- employ unit or personnel in charge of information security;
- use information processing program, network and equipment that are approved by the authorized entity;
- use licensed program in order to prevent information security risks and conduct an information security evaluation every two years or when necessary;
- conduct an information security audit on an annual basis; and
- maintain historical records of information changes, deletions, and restorations, and monitor and ensure the integrity and confidentiality of the information.

The Information Security Requirement further requires that the information processing server of the Data Controller must:

- be located in the territory of Mongolia;
- be accessible only from Mongolia;
- be placed in the dedicated technical room;
- be able to increase the capacity of the server if necessary;
- be able to exchange information through the state information exchange system "KHUR";
- be connected to the network time server of the Communications Regulatory Commission of Mongolia;
- be protected by "SSL" certificate; and
- be able to be backed up on a regular basis.

The Cyber Security Law of Mongolia, adopted by the Parliament on 17 December 2021 regulates matters pertaining to the establishment of systems, principles and legal framework for ensuring cyber security. According to the Cyber Security Law, “cyber security system” that is responsible for ensuring cyber security includes the Government, intelligence agency, state-owned legal entities, police organization, citizens, legal entities and entities with critical information infrastructure, such as entities operating in the energy, health and payment sectors, as well as database operators and border ports. For instance, the Law provides that an individual person must be responsible for maintaining cyber security of himself and individuals under his or her care.

BREACH NOTIFICATION

The Data Protection Law states that data collector must promptly notify the Data Controller of any breaches occurred during the data collection and processing. If such breach has potential to cause damages to the rights and legitimate interest of the Data Owner, the Data Controller must immediately provide notice to the Data Owner including the following:

- the Data Owner who will be affected by the breach;
- name and contact information of the Data Controller;
- possible negative consequences from the breach; and
- measures taken to eliminate potential negative consequences from the breach.

ENFORCEMENT

Since the adoption of the Data Protection Law, the General Intelligence Agency of Mongolia, as ordered by the Prime Minister of Mongolia, has been organizing and supervising the deletion of non-overlapping body data (i.e. fingerprints), which was collected by, compiled by or registered with any person other than the Data Controller. Deletion of fingerprints concerns (i) Data Controllers with fingerprint data stored at and connected to the "KHUR" system of the state information exchange, (ii) public and private legal entities that register the check-in or work hours of employees using fingerprints without permission, and (iii) those who use fingerprints for the purposes of exercising other rights and obligations.

As set forth in the Data Protection Law, the Ministry of Digital Development and Communications and the National Human Rights Commission are responsible for the enforcement of the Data Protection Law and will investigate an act or practice if such act or practice may be (i) a violation of the privacy of an individual and (ii) a complaint about the act or practice have been submitted. Pursuant to the Data Protection Law, the Data Owner can submit a claim to the administrative courts or the competent authority as provided under the relevant laws with respect to its complaint on the data collection, processing and use by the state authority. Complaints on data collection, processing and use by the other Data Controllers can be submitted to the other authorised entity or the Human Rights Commission.

Any breach or violations of the Data Protection Law is subject to sanctions under the Violations Law or the Criminal Code of Mongolia. For instance, use of Personal Data against the lawful purposes or the initial permit provided by the Data Owner is subject to a monetary fine in the amount of MNT 500,000 (approx. USD 147) for individuals and MNT 5,000,000 (approx. USD 1,466) for legal entities. Creation of a condition that results in a breach of freedom and legitimate rights of the Data Owner due to a processing of Personal Data in the electronic form without the human interference will also be a subject to monetary fine in the amount of MNT 500,000 (approx. USD 147) for individuals and MNT 5,000,000 (approx. USD 1,466) for legal entities. Illegal collection, processing and transfer of the Personal Data that is not subject to a criminal liability is subject to a monetary fine in the amount of MNT 2,000,000 (approx. USD 586) for individuals and MNT 20,000,000 (approx. USD 5,866) for legal entities.

ELECTRONIC MARKETING

There are no specific provisions under the Data Protection Law or other Mongolian laws regulating electronic marketing communications. It is important to point out, however, that, according to the Data Protection Law, all processing of consumer Personal Data (which includes the collection, storage and making available to the public) can only occur upon the appropriate legal basis for such purpose and permission provided by the Data Owner.

ONLINE PRIVACY

Currently, there are no laws or regulations in Mongolia regulating online privacy, including cookies and location data. Although the Data Protection Law does not address online privacy including cookies and location data, the Ministry of Digital Development and Communications, within the authority entitled to it under the Data Protection Law and other relevant laws, may adopt regulations concerning the storage, use, disclosure and other processing of data collected on the internet.

KEY CONTACTS

DB&GTS LLP
dblaw.mn/

Ariunbayar Enkhbat
Senior Associate
DB&GTS LLC
T +976 880 06058
e.ariunbayar@dblaw.mn

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MONTENEGRO

Last modified 18 January 2024

LAW

The Law on Protection of Personal Data, Official Journal of Montenegro, nos. 79/2008, 70/2009, 44/2012 and 22/2017, (DP Law) is the governing data protection law. It was first enacted in December 2008 and last amended in April of 2017.

The Montenegrin Parliament is expected to adopt a new Data Protection Law to harmonize its data protection law with the EU General Data Protection Regulation (GDPR). However, there is no certainty when exactly, i.e. within which timeframe such adoption (and further implementation) should occur.

DEFINITIONS

Definition of personal data

The DP Law defines personal data as any information relating to an identified or identifiable data subject. Data subjects are natural persons whose identity is or can be determined, directly or indirectly, in particular by reference to a personal identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

Under the DP Law, sensitive personal data is data relating to:

- Ethnicity or race
- Political opinion, or religious or philosophical belief
- Trade union membership
- Information on health condition and sexual life

NATIONAL DATA PROTECTION AUTHORITY

The Agency for Protection of Personal Data and Free Access to Information (**DPA**) is the local data protection authority. The DPA is currently located at:

Bulevar revolucije 11
Podgorica

Website

www.azlp.me

REGISTRATION

Each data controller must do the following:

- Register as a data controller (this registration as a controller is to be performed only once);
- Separately register each database of personal data ('Database') which it intends to establish, before the database is established.

Both registrations must be submitted online through specific forms, whereas the database's registration form is accessible via the DPA's website. The type and scope of the information that must be included in these forms is explicitly prescribed by the DP Law (e.g. the data controller's name and address of its registered seat, name of the Database, legal basis for the processing and purpose of the processing, types of processed data, categories of data subjects, (if applicable) information on any data transfers out of Montenegro). Any significant change to the registered data processing activities, subsequent to the registration should be notified to and registered with the DPA as well.

Exceptionally (i.e. if the intended data processing represents a special risk for the rights and freedoms of individuals), a data controller may, depending on the circumstances of each particular case, be obliged to obtain the DPA’s prior approval for such processing (e.g. if biometric data is to be processed without the data subject's consent).

DATA PROTECTION OFFICERS

Under the DP Law, a data controller is required to appoint a DPO subsequent to the Database's establishment. However, a DPO is not required if the data controller has less than ten employees involved in the processing of personal data.

COLLECTION & PROCESSING

A prerequisite for the legitimate processing of personal data is to obtain the data subject’s valid, informed consent. The consent requirements are explicitly described in the DP Law (e.g. data subjects have to be informed about the purpose and legal basis for the respective processing). The processing of personal data without consent is only allowed under the exceptions listed in the DP Law, (e.g. if the processing is necessary to meet the data controller's statutory obligations under the law or for the protection of life and other vital interests of the data subject who is not capable to personally consent).

As a general matter, in order to comply with the provisions under the DP Law, the processing has to be done in a fair and lawful manner, the type and scope of processed data must be proportionate to the purpose of the respective processing, the data should not be retained longer than necessary in order to meet the defined purpose, and the data has to be accurate, complete and up-to-date.

TRANSFER

Under the DP Law, personal data may be transferred to countries or international organizations, where an adequate level of personal data protection exists, subject to the DPA's approval. The DPA issues such approval only where it establishes that adequate measures for the protection of personal data are undertaken (criteria for the adequacy assessment include, for example, the type of the data and the statutory rules in force in the country to which the data is to be transferred).

However, in certain cases the DPA's approval is not required for data transfers out of Montenegro, as explicitly prescribed by the DP Law (e.g. if the data subject consented to the transfer and was made aware of possible consequences of such transfer, or the data is transferred to the European Union or European Economic Area or to any country that the EU Commission has determined ensure adequate level of the data protection).

SECURITY

The DP Law requires that both data controllers and processors undertake technical, personnel and organizational measures for the protection of personal data against loss, destruction, unauthorized access, alteration, publication and misuse. Further, individuals who process personal data are required to keep the processed personal data confidential.

Additionally, data controllers are required to establish internal rules regarding their personal data processing and protection of same (which should include identifying the measures undertaken). Data controllers should also determine which employees have access to the processed data (and to which of this data), as well as the types of data which may be disclosed to other users (and the conditions for the respective disclosure). Finally, if the processing is performed electronically, a data controller is required to ensure that certain information on the use and recipients of the respective data, is automatically kept in the information system.

BREACH NOTIFICATION

There is no data security breach notification requirement under the DP Law. However, the Law on Electronic Communications ('Official Journal of Montenegro', nos. 40/2013, 56/2013, 2/2017 and 49/2019) ('EC Law') does impose a duty on operators to, without undue delay, notify the Montenegrin Agency for Electronic Communications and Postal Activity (EC Agency) and the DPA of any breach of personal data or privacy of the data subjects. The affected data subject should also be notified if the breach may have a detrimental effect to their personal data or privacy (unless the EC Agency issues an opinion that such notification is not needed). Failure to comply with any of the above duties is subject to liability and fines, ranging from EUR 6,000 to EUR 30,000 for a legal entity, and from EUR 300 to EUR 3,000 for a responsible person within a legal entity, and, if some material gain was obtained through the violation, the protective measure, which includes seizure of the respective gain, may be imposed in addition to the above monetary fine.

ENFORCEMENT

The DPA is the competent authority for the DP Law's enforcement. It is authorized and obliged to monitor implementation of the DP Law, both ex officio, and upon a third-party complaint.

When monitoring the DP Law's implementation, the DPA is authorized to pass the following decisions:

- Order removal of the existing irregularities within certain period of time;
- Temporarily ban the processing of personal data which is carried out in violation of the DP Law;
- Order deletion of unlawfully collected data;
- Ban transfer of data outside of Montenegro or its disclosure to data recipients carried out in violation of the DP Law;
- Ban data processing by an outsourced data processor if it does not fulfil the data protection requirements or if its engagement as a data processor is carried out in contravention to the DP Law.

The DPA's decisions may not be appealed, but an administrative dispute before the competent court may be initiated against the same.

The DPA may also file a request for the initiation of offence proceeding before a competent Montenegrin court. The offenses and sanctions are explicitly prescribed by the DP Law, which includes monetary fines ranging from €500 to €20,000 for a legal entity and ranging from €150 to €2,000 for a responsible person in a legal entity.

There exists potential criminal liability. The unauthorized collection and use of personal data is a criminal offense under the Montenegrin Criminal Code, punishable with a fine (in an amount to be determined by the court) or imprisonment up to one year (i.e. up to three years if committed by a public official / state servant when performing his duties). Both natural persons and legal entities can be subject to criminal liability.

ELECTRONIC MARKETING

Electronic marketing is not governed by the DP Law. Nevertheless, this law does govern protection of personal data used in direct marketing. In that regard, the law requires that data subjects have to be provided with a possibility to object to the processing of their personal data for direct marketing purposes prior to the commencement of the respective processing. Regarding the use of sensitive personal data in direct marketing, it is explicitly prescribed that a data subject's consent is a requirement for the respective processing.

Although not governed by the DP Law, there are other regulations which govern electronic marketing, including the Law on Electronic Trade ('Official Journal of the Republic of Montenegro', no. 80/04 and 'Official Journal of Montenegro', nos. 41/10, (…), 56/13) ('ET Law'). In this respect, one of the most important rules prescribed by the ET Law is the rule that any

sending of unsolicited commercial messages is not allowed unless prior consent of the recipients of the respective marketing is obtained. It is strictly forbidden to send any marketing messages to individuals who have indicated that they do not want to receive such (i.e. opted-out) (and a service provider who sends unsolicited commercial messages is required to establish and maintain a record of individuals who opted-out). A violation of the respective rules is subject to liability, with fines ranging from EUR 500 to EUR 17,000 (for a legal entity) and ranging from EUR 100 to EUR 1,500 (for a responsible person in a legal entity). For particularly serious violations or repeated violations, an order banning or suspending the business activity (lasting from three months to six months) may be imposed on an entity responsible for the respective violations).

ONLINE PRIVACY

There is no specific law or regulation explicitly governing online privacy, including cookies. Accordingly, the general data protection rules, as introduced by the DP Law, are applicable to online privacy, to the extent personal data is processed.

On the other hand, the EC Law, as defined in Breach notification, introduces relevant rules that are mandatory for the operators under this law. For example, a public electronic communication services' user is particularly entitled to the protection of their electronic communications' secrecy in compliance with the DP Law.

Further, the EC Law imposes explicit rules on traffic data and location data. Under these rules, operators are:

- Required to retain certain traffic data and location data for certain purposes explicitly set out by the law (for example, for the detection and criminal prosecution of criminal offenders), whereas the retention period should last at least six months and would not be longer than two years ('Retention Obligation'), keeping in mind that this obligation does not apply to data which reveals a content of electronic communications.
- Regarding traffic data related to subscribers / users which is not subject to the Retention Obligation, an operator is required to delete this data if it is no longer needed for the communication's transmission or can keep it, but only if it modifies the respective data in a way that it cannot be linked to a particular person. Apart from this, it is also prescribed that:
    - If the traffic data's retention purpose is to use it for the calculation of the costs of the relevant services / interconnection, it can be retained for as long as claims regarding the respective costs can legally be requested, but under condition that an user is informed on its processing's purpose and duration; and that
    - If the traffic data's processing purpose is to promote and sell electronic communication services or to provide value added services, such processing is allowed, but only with the data subjects' prior consent (which can be withdrawn at any time).
- Regarding location data which is not subject to the Retention Obligation, an operator is allowed to process it but only with the data subject's consent (which can be withdrawn at any time) or if the respective data is modified in a way that it cannot be linked to a particular person without consent.

Failure to comply with any of the above rules regarding the processing of traffic or location data which is not covered by the above-identified Retention Obligation, is subject to offence liability and fines in range from EUR 4,000 to EUR 20,000 for a legal entity, and in range from EUR 200 to EUR 2,000 for a responsible person in a legal entity.

KEY CONTACTS

Karanovic & Nikolic
www.karanovic-nikolic.com/

Sanja Spasenović
Attorney at Law in cooperation with Karanović & Partners
Karanovic & Partners
T +381 11 3094 200/ +381 11 3955 413
sanja.spasenovic@karanovicpartners.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MOROCCO

Last modified 18 January 2024

LAW

Morocco’s law governing privacy and data protection is Law No 09-08, dated February 18, 2009 relating to protection of individuals with regard to the processing of personal data and its implementation Decree n° 2-09-165 of May 21, 2009 (together the DP Law).

DEFINITIONS

Definition of personal data

Pursuant to Article 1 of the DP Law, personal data is defined as any information regardless of their nature, and format, relating to an identified or identifiable person.

Definition of sensitive personal data

Sensitive personal data is defined under the law as personal data which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs or union membership of the person concerned or relating to his health, including his genetic data (article 1.3 of the DP Law).

NATIONAL DATA PROTECTION AUTHORITY

The relevant authority is the Data Protection National Commission (*Commission Nationale de Protection des Données Personnelles*).

REGISTRATION

The processing of personal data is subject to:

- A prior declaration to be filed with the Moroccan Data Protection Commission; or
- A prior authorization of the Moroccan Data Protection Commission when the processing concerns any of the following:
    - Sensitive data (e.g. revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, including genetic data);
    - Using personal data for purposes other than those for which they were initially collected;
    - Genetic data, except for those used by health personnel and that respond to medical purposes;
    - Data relating to offenses, convictions or security measures, except for those used by the officers of the court;
    - Data which includes the number of the national identity card of the concerned person.

The declaration and authorization includes a commitment that the personal data will be treated in accordance with the DP Law.

The prior declaration and authorization shall include, without limitation, the following information:

- The name and address of the person in charge of the processing and, if applicable, its representative;
- The name, characteristics and purpose(s) of the intended processing;
- A description of the category or categories of data subjects, and the data or categories of personal data relating thereto;
- The recipients or categories of recipients to whom the data are likely to be communicated;
- The intended transfers of data to foreign states;
- The data retention time;
- The authority with which the data subject may exercise, if any, the rights granted to him / her by law, and the measures taken to facilitate the exercise of these rights;
- A description of the confidentiality and security measures in place to protect personal data; and
- Overlap, interconnections, or any other form of data reconciliation and their transfer, subcontracting, in any form, to third parties, free of charge or for consideration.

DATA PROTECTION OFFICERS

There is no requirement for a data protection officer under the DP Law.

COLLECTION & PROCESSING

The personal data must be processed in accordance with the following principles:

- Treated fairly and lawfully;
- Collected for specific, explicit and legitimate purposes;
- Adequate, relevant and not excessive;
- Accurate and necessary and kept up-to-date;
- Kept in a form enabling the person concerned to be identified.

As a general rule, the processing of a personal data must be subject to the prior consent of the relevant data subject.

While the applicable regulations provide that the processing of personal data can be performed without the consent of the relevant data subject in some specific instances, the Moroccan Data Protection Commission rarely accepts that the data controllers process personal data without the consent of the relevant data subject.

TRANSFER

Prior authorization from the National Commission is required before any transfer of personal data to a foreign state.

Further, the person in charge of the processing operation can transfer personal data to a foreign state only if the said state ensures under its applicable legal framework an adequate level of protection for the privacy and fundamental rights and freedoms of individuals regarding the processing to which these data is or might be subject, unless:

- The data subject has expressly consented to the transfer
- The transfer and subsequent processing is required for:
    - Compliance with a legal obligation to which the concerned person or the person in charge of the processing are submitted
    - The execution of a contract to which the concerned person is party or in the performance of pre-contractual measures taken at the request of the latter
    - The protection of the vital interests of the relevant data subject, if that person is physically or legally unable to give its consent
    - Performance of a task of public interest or related to the exercise of public authority, vested in the person in charge of the processing or the third party to whom the data are communicated

- Fulfillment of the legitimate interests pursued by the data controller or by the recipient, when not outweighed by the interests or fundamental rights and freedoms of the relevant data subject

In practice, we notice that CNDP interprets the exception of legitimate interests of the data processor very restrictively. CNDP is in general more comfortable relying on the data subject’s consent regarding any transfers to a foreign state.

SECURITY

Article 23 of the DP Law provides that an organization is required to implement all technical and organizational measures to protect personal data in order to prevent it being damaged, altered or used by a third party who is not authorized to have access, as well as to protect it against any form of illicit processing.

Additionally, in appointing processors and subcontractors an organization must choose a processor or subcontractor who provides sufficient guarantees with regard to the technical and organizational measures relating to the processing to be carried out while ensuring compliance with these measures.

BREACH NOTIFICATION

There is no requirement for a data protection officer under the DP Law, except, where relevant, through the application of GDPR.

ENFORCEMENT

The Data Protection National Commission enforces compliance of the DP Law.

Article 50 to 64 provide that non-compliance with the DP Law is punishable by a fine ranging from DH10,000 to DH600,000 and / or imprisonment between three months and four years.

If the offender is a legal person, and without prejudice to the penalties which may be imposed on its officers, penalties of fines shall be doubled.

In addition, the legal person may be punished with one of the following penalties:

- The partial confiscation of its property
- Seizure of objects and things whose production, use, carrying, holding or selling is an offense
- The closure of the establishment(s) of the legal person where the offense was committed

ELECTRONIC MARKETING

Direct marketing by means of an automated calling machine, a fax machine, email or a similar technology, which uses, in any form whatsoever, an individuals' data without their express prior consent to receive direct prospecting is prohibited.

However, direct marketing via email may be allowed if the recipient’s email address has been received directly from him / her.

In the absence of consent, unwanted emails can only be sent if all of the following conditions are satisfied:

- The contact details were provided in the course of a sale
- The marketing relates to a similar product

- The recipient was given a method to opt out of the use of their contact details for marketing when they were collected

ONLINE PRIVACY

The general data protection principles under the DP Law apply.

KEY CONTACTS

Mehdi Kettani
Head of IPT
T +212 (0) 660 16 44 56
Mehdi.Kettani@dlapiper.com

Adil Mouline
Lawyer
T +212 (0) 620 57 00 00
Adil.Mouline@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MOZAMBIQUE

Last modified 18 January 2024

LAW

In Mozambique there is no specific legislation on data protection or privacy. However, there are other sources of law that impose some privacy obligations, including:

- The Civil Code (Decree-Law no. 47344, of November 25, 1966, in force in Mozambique through Edict no. 22869, dated September 4, 1967);
- The Penal Code (Law no. 24/2019, of December 24, as amended by Law no. 17/2020 of 23 December);
- The Labour Law (Law no. 23/2007, of August 1) and the new Labour Law (Law no. 13/2023, of 25 August) which enters into force on 22 February 2023;
- The Electronic Transactions Law (Law no. 3/2017, of January 9);
- The Regulations on Registration and Licensing of Intermediary Electronic Service Providers and Operators of Digital Platforms (Decree no. 59/2023, of 27 October); and
- Resolution no. 5/2019, of 20 June, ratifies the African Union Convention on Cybersecurity and Personal Data Protection (“AU Convention”).

In addition, the Constitution of the Republic of Mozambique provides that all citizens are entitled to the protection of their private life and have the right to honor, good name, reputation, protection of their public image and privacy. Further, Article 71 of the Constitution identifies the need to legislate on access, generation, protection and use of computerized personal data (either by public or private entities); however, implementing legislation has not yet been approved.

DEFINITIONS

Definition of personal data

The Electronic Transactions Law defines personal data as being any information in relation to a natural person which can be directly or indirectly identified by reference to an identification number or one or more factors. The AU Convention contains an indication of these factors, being: physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

The Constitution of the Republic of Mozambique imposes restrictions on recording and handling any individually identifiable information concerning a person’s political, philosophical or ideological beliefs, religious beliefs, membership in a political party or trade union and (particulars) related to the person’s privacy. In addition, the AU Convention also considers personal data relating to sex-life, race, health, social measures, legal proceedings and penal or administrative sanctions as sensitive.

NATIONAL DATA PROTECTION AUTHORITY

There is no data protection authority in Mozambique but the National Institute of Information and Communications Technology (*Instituto Nacional de Tecnologia de Informação e Comunicação* – “**INTIC**”) has some competencies in this regard.

The Cybersecurity Bill will establish INTIC as the national cybersecurity authority, insofar as it relates to electronic communications.

REGISTRATION

Decree 59/2023 requires the registration of Intermediate Electronic Services Providers and Operators of Digital Platforms. The Electronic Transactions Law defines the intermediate service provider as any person who, in representation of another, sends, receives and stores data messages, and also who provides network access services or provide services through a network. Any entity that performs such acts will qualify as an intermediate service provider and must be registered and licensed with INTIC.

The registration requirement is applicable to Intermediate Electronic Services Providers and Operators of Digital Platforms that offer services to receivers based or located in Mozambique, regardless of where the providers are based.

DATA PROTECTION OFFICERS

The Electronic Transactions Law requires the data processor to appoint someone responsible for compliance of the provisions related to electronic personal data protection.

COLLECTION & PROCESSING

Under the Constitution of the Republic of Mozambique, individually identifiable information, concerning political, philosophical or ideological beliefs, religious beliefs, membership in a political party or trade union and (particulars) related to the person’s privacy may not be stored or processed in a database.

TRANSFER

The law does not generally restrict cross-border transfers of personal information. The Constitution of the Republic of Mozambique imposes restrictions on disclosures of personal information to third parties, unless prior consent from the data subject is obtained.

Although there is a prohibition against the transfer of personal data to a non-Member State under the AU Convention, this prohibition does not apply if said State ensures adequate level of protection of the privacy, freedoms and fundamental rights of the data subject. The AU Convention also requires that consent be sought from the national protection authority before the data controller may transfer the data to a third country. Currently, INTIC does not have such powers so the principle of consent of the data subject and the transfer of data to a country with an adequate data protection framework would apply. Notwithstanding, parties may approach INTIC for further guidance on this matter.

SECURITY

Under the Electronic Transactions Law, the person / entity responsible for processing electronic data, must protect personal data against risks, losses, unauthorized access, destruction, use, modification or disclosure.

The Cybersecurity Bill also establishes a duty on data processors and data controllers to ensure the confidentiality of data stored in electronic communications network.

BREACH NOTIFICATION

There is currently no breach notification requirement in Mozambique.

A Cybersecurity Bill is being discussed which intends to establish amongst other things, the legal regime applicable to the protection of data communication networks, of data, of information systems and critical infrastructures in cyberspace.

The bill stipulates which entities are required to notify in the event of a data breach.

ENFORCEMENT

Under the Electronic Transactions Act, a violation of the data protection duty or the duties of a data processor is subject to a fine of between 30 to 90 minimum wage salaries in effect in the public administration sector, in the absence of a more serious punishment.

The Penal Code (Law no. 24/2019 of December 24, as amended by Law no. 17/2020 of December 23) provides for certain cybercrimes, such as intrusion of automatized database, which is subject to imprisonment of up to two years and corresponding fine. There are also other cybercrimes such as fraud through electronic means and unauthorized use of data resulting in unjust enrichment, which is subject to imprisonment generally from a year up to five years and a corresponding fine. The new Penal Code attempts to bridge the gap by identifying cybercrimes related to data protection which are punishable.

The Cybersecurity Bill also makes provision for fines and sanctions for the violation of its provisions.

However, given that Mozambique does not have specific data protection laws nor a specific authority responsible for overseeing data protection matters, enforcement of data protection-related matters is minimal.

ELECTRONIC MARKETING

The rules applicable to electronic advertisement and marketing are provided under the Advertisement Code (Decree no. 38 /2016, of August 31) and the Electronic Transactions Law (Law no. 3/2017, of January 9).

Under the Electronic Transactions Law, express consent from a recipient is required prior to sending direct marketing communications via automated dialing systems, fax machines and email, unless one of the following applies

- If the sender obtained the contact details of the recipient during the sale or negotiations for the sale of a product or service to the recipient;
- The direct marketing refers to similar products or services to those of the recipient;
- At the moment of initial collection of the data, the recipient was offered the option to refuse of use of his contact details, and decided not to refuse;
- If the recipient did not refuse the use of its data in any subsequent communications.

Under the Advertisement Code, electronic marketing messages should be clearly identified and include sufficient information, so as to allow the common recipient to easily understand all of the following:

- The nature of the message;
- The advertiser;
- The promotional offers, such as discounts, prizes, gifts and promotional contests and games, as well as the conditions to which they are bound (if applicable).

All direct marketing message must provide recipients with information about how to opt out of further marketing communications, as well as the identity details of the source from which the contact details of the consumer have been obtained.

ONLINE PRIVACY

Other than the above general rule, there are no other rules applicable to online privacy.

However, the Cybersecurity Bill intends to establish the duty to ensure the integrity, confidentiality and privacy of the information systems during the communication of data using the internet.

KEY CONTACTS

Eduardo Calu

Managing Partner
SAL & Caldeira Advogados, Lda.
T +258 21 241 400
ecalu@salcaldeira.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

MYANMAR

Last modified 2 January 2024

LAW

There is no general data protection law in Myanmar. Relevant laws on data protection and privacy can be found in various legislation, which include:

- Financial Institutions Law (2016);
- Telecommunications Law (2013);
- Notification 116/97 of the Ministry of Finance and Revenue;
- Law Relating to Private Health Care Services (2007); and
- Electronic Transactions Law (2004) and its 2021 amendment.

DEFINITIONS

Definition of Personal Data

Personal Data means any information that relates to an identified or identifiable living individual. (Section 2(l) of Electronic Transaction Law as amended in 2021).

Definition of Sensitive Personal Data

No definition provided.

NATIONAL DATA PROTECTION AUTHORITY

None.

REGISTRATION

N/A

DATA PROTECTION OFFICERS

There is no definition of Data Protection Officers, but there is a definition for Personal Data Administrator. The Personal Data Administrator (“**PDA**”) means “a person and its staff authorized by a government department or an entity having power to conduct the collecting, storing and using of personal data according to the provision of this law or any existing law.” (Section 2(m) of Electronic Transaction Law as amended in 2021).

COLLECTION & PROCESSING

By implication from relevant laws, collection and processing of personal data requires consent.

TRANSFER

By implication from relevant laws, transfer of personal data requires consent.

SECURITY

By implication from relevant laws, personal data must be kept with reasonable security arrangements.

BREACH NOTIFICATION

No obligation.

ENFORCEMENT

None so far as at January 2, 2024.

ELECTRONIC MARKETING

There is no specific law. However, electronic marketing would generally be governed by the Competition Law (2015) and the Consumer Protection Law (2019).

ONLINE PRIVACY

There is no specific law. However, the Law Protecting the Privacy and Security of Citizens (2017), Electronic Transactions Law and E-Commerce Guidelines (2023) deal with privacy of communications and personal data.

KEY CONTACTS

Nwe Oo
Senior Associate
Tilleke & Gibbins
T +95 772 440 001
nweoo@tilleke.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

NAMIBIA

Last modified 18 January 2024

LAW

Namibia recognises the right to privacy as a fundamental human right under Article 13 of the Namibian Constitution. Accordingly, all persons have a right to privacy in their homes and communications. The right to privacy is limited as required by law and in the interest of protecting:

- national security and public safety;
- the nation’s economy;
- health and morals;
- against disorder and crime;
- the rights and freedoms of others.

Save for the constitutional right to privacy, Namibia has not enacted comprehensive data privacy legislation. However, various sector-specific laws are in place to protect client information, including in the legal and banking sectors.

The Namibian Government has published the Draft Data Protection Bill, 2021. The objectives of this draft Bill are to:

- establish a Data Protection Supervisory Authority and to provide for its powers, duties and functions;
- establish obligations of data controllers and processors;
- make provision for the regulation of the processing of information relating to individuals in order to protect the fundamental rights and freedoms of individuals, and in particular, their right to privacy concerning the processing of such information;
- provide for the rights of individuals about whom information is processed;
- provide for restrictions and exceptions under the provisions of this Act; and
- provide for codes of conduct of controllers and processors and for matters connected therewith.

DEFINITIONS

Definition of Personal Data

Not defined.

Definition of Sensitive Personal Data

Not defined.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in Namibia.

REGISTRATION

There is no registration requirement.

DATA PROTECTION OFFICERS

MICT

COLLECTION & PROCESSING

There are no restrictions on the collection and processing of personal data.

TRANSFER

There are no data transfer restrictions in place.

SECURITY

There are no data security requirements.

BREACH NOTIFICATION

There are no requirements to report data breaches to any individual or regulatory body.

ENFORCEMENT

There is no enforcement mechanism in place.

ELECTRONIC MARKETING

There are no electronic marketing regulations.

ONLINE PRIVACY

There are no specific laws that regulate the manner in which personal data may be stored or transmitted online.

KEY CONTACTS

Peter Johns
Director
Ellis Shilengudwa Incorporated
T +264 61 242224
peter@esinamibia.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

NEPAL

Last modified 29 December 2022

LAW

1. Individual Privacy Act, 2018 (2075) (“**Privacy Act**”)
2. Individual Privacy Regulation, 2020 (2077) (“**Privacy Regulation**”)
3. National Penal Code, 2017 (2074) (“**Penal Code**”)
4. Advertisement Act, 2019 (2076) (“**Advertisement Act**”)
5. Advertisement Regulation, 2020 (2076) (“**Advertisement Regulation**”)
6. National Broadcasting Regulation 1995 (2052) (“**National Broadcasting Regulation**”)

DEFINITIONS

Definition of Personal Data

Privacy Act defines "Personal information" as the following information related to any person:

- his or her caste, ethnicity, birth, origin, religion, color or marital status;
- his or her education or academic qualification;
- his or her address, telephone or address of electronic letter (email);
- his or her passport, citizenship certificate, national identity card number, driving license, voter identity card or details of identity card issued by a public body;
- a letter sent or received by him or her to or from anybody mentioning personal information;
- his or her thumb impressions, fingerprints, retina of eye, blood group or other biometric information;
- his or her criminal background or description of the sentence imposed on him or her for a criminal offence or service of the sentence;
- matter as to what opinion or view has been expressed by a person who gives professional or expert opinion, in the process of any decision.

Definition of Sensitive Personal Data

Privacy Act has listed following information as the “sensitive information”:

- his or her caste, ethnicity or origin;
- political affiliation;
- religious faith or belief;
- physical or mental health or condition;
- dexual orientation or event relating to sexual life;
- fetails relating to property.

NATIONAL DATA PROTECTION AUTHORITY

Not applicable.

REGISTRATION

Not applicable.

DATA PROTECTION OFFICERS

Not applicable.

COLLECTION & PROCESSING

Collection

The collection of data by any public body or body corporate is allowed with the consent of the concerned person. In addition to this, the Privacy Act provides an exclusive provision in the context of the collection of data. It provides that no one except the official authorized under law or the person permitted by such official shall collect, store, protect, analyze, process or publish the personal information of any person. Officer authorized under the law means those officials who have been authorized by other laws to collect the information such as investigating authority, collection of prescribed information by the civil service officer.

Processing

Privacy Act prohibits to process the sensitive information. However, the sensitive information can also be processed in following circumstances:

- in the course of alleviation of disease, public health protection, disease identification, health treatment, management of health institution and providing health service by the health worker, without insulting or letting the concerned person feel inferior;
- if the concerned person has published the information himself or herself.

TRANSFER

The 11th amendment to National Broadcasting Regulation which has been effective from 3rd March 2022, has mandated Over the Top ("**OTT**") service providers to store their customer data within servers in Nepal. Such requirements only extend to OTT service providers and the regulation has defined OTT as “*the service of delivering any program according to the consumer's demand through the internet and without the use of cable or satellite television, and the term also refers to media streaming services on other platforms via the internet.*” However, the National Broadcasting Regulation is silent on the methods / procedure / requirements for the transfer of such data outside Nepal.

Furthermore, the Information Technology Bill, 2019 (2075) (which is currently tabled in the parliament of Nepal), if implemented in its current form, then the prescribed data held by governmental, public, financial, and health-related authorities would be prohibited for export outside Nepal. Also, Bill to amend Record Protection Act 1989 (2046) would further prohibit to export records of national importance outside Nepal.

SECURITY

The collected data should only be used for the purpose for which such data have been collected. Further, the Privacy Act obligates the public body which has the collected information, to make appropriate arrangements for the protection of collected information.

BREACH NOTIFICATION

Not applicable.

ENFORCEMENT

As aforementioned, the prevailing laws have not designated Data Protection Authority. Nonetheless, the Privacy Act and Criminal Code provide a complaint mechanism.

Complaint of the offense under the Privacy Act is processed either by filling a plaint at the concerned district court by the concerned person or filling FIR at the relevant police office. In relation to the latter one, the concerned police office through the government office would file a charge sheet in the concerned district court. Such procedure of directly filing a complaint at the concerned district court or police office is determined based on the nature of the offense. In relation to an offense under the Criminal Code, the FIR process as aforementioned is adopted.

ELECTRONIC MARKETING

The matters related to marketing are regulated by the Advertisement Act and Advertisement Regulation. The definition as provided under the Advertisement Act also includes inter alia advertisement done through electronic medium, online or social media.

Advertisement-oriented SMS or Email cannot be sent to any person without obtaining the said concerned person’s consent.

ONLINE PRIVACY

Every person has the right to privacy in terms of data available in electronic means. Such data cannot be used or share such data without the consent of the concerned person. In relation to the cookies and location data, there is no exclusive provision for it. However, if a data subject’s personal information or location data is collected using cookies or otherwise, the concerned entity must adhere to the Privacy Act and further such information must be used for the same purpose as it was collected for.

KEY CONTACTS

Pioneer Law Associates
pioneerlaw.com/

Anup Raj Upreti
Managing Partner
Pioneer Law Associates
T +977-980165418
anup@pioneerlaw.com

Suman Siwakoti
Associate
Pioneer Law Associates
T +977-9801079825
suman@pioneerlaw.com

Sujan Shrestha
Associate
Pioneer Law Associates
T +977-9801109841
sujan.shrestha@pioneerlaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

NETHERLANDS

Last modified 18 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The Dutch GDPR Implementation Act (*Uitvoeringswet AVG*, the **Implementation Act**) constitutes the local implementation of the GDPR in the Netherlands. The Implementation Act follows a policy-neutral approach, meaning that the requirements of the previous Dutch Data Protection Act (*Wet bescherming persoonsgegevens*) are maintained insofar as possible under the GDPR. The Implementation Act provides for, among other things, national rules where this is necessary for the implementation of GDPR provisions on the position of the regulatory authority or the fulfilment of discretionary powers provided by the GDPR. There is a pending legislative proposal, the Data Protection Collection Act (*Verzamelwet gegevensbescherming*), that will affect the Implementation Act on a few specific topics. For example, adjustments will be made to the definition of criminal data and the existing derogations under the Implementation Act for the processing of biometric data will be further conditioned.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions are largely the same as in Article 4, GDPR. In addition, the Implementation Act defines "personal data concerning criminal law matters" as personal data concerning criminal convictions and offences or related security measures as referred to in Article 10, GDPR, as well as personal data relating to a prohibition imposed by the courts for unlawful or objectionable conduct.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the DPC in Ireland). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) has been appointed by law as the supervisory data protection authority and supervises compliance with the GDPR and the Implementation Act.

The Dutch Data Protection Authority's contact details are as follows:

Autoriteit Persoonsgegevens
Postbus 93374
2509 AJ DEN HAAG

Telephone number

(+31) - (0)70 - 888 85 00

Website

autoriteitpersoonsgegevens.nl

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale
- Its core activities consist of processing sensitive personal data on a large scale

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have expert knowledge (Article 37(5)) of data protection laws and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff

- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The Implementation Act (Article 39) provides more detailed information regarding the secrecy requirement set out in Article 38(5) GDPR, by stipulating that the DPO must maintain the secrecy of any information that becomes known to him or her pursuant to a complaint by or request from a data subject, unless the data subject agrees to disclosure.

Organisations must register their DPO with the Dutch Data Protection Authority *(Autoriteit Persoonsgegevens)*. The registration form is available here.

A special email address and phone number is available for registered DPOs to contact the Dutch Data Protection Authority in case of questions with regard to the tasks of DPOs and GDPR compliance.

The contact details are as follows:

Email address: FG@autoriteitpersoonsgegevens.nl

Phone number: (+31) (0)70-8888660

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to demonstrate compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time)

- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected

- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision taking, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. Necessary for entering into or performing a contract
b. Authorized by EU or Member State law
c. The data subject has given their explicit (i.e. opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Special categories of personal data (Article 9)

Article 9(2) of the GDPR provides for a number of exceptions under which special categories of personal data may lawfully be processed. Certain of these exceptions require a basis in Member State law.

Division 3.1 of the Implementation Act provides for various exceptions for the processing of different types of special categories of personal data, subject to stringent conditions. Important examples include exceptions for:

- Scientific or historical research or statistical purposes
- The processing of personal data revealing racial or ethnic origin
- The processing of personal data revealing political opinions for the performance of public duties

- The processing of personal data revealing religious or philosophical beliefs for spiritual care
- Genetic, biometric and health data

Criminal convictions and offences data (Article 10)

The processing of criminal conviction or offences data is prohibited by Article 10 of the GDPR, except where specifically authorized under relevant Member State law.

Division 3.2 of the Implementation Act provides several exceptions for the processing of criminal convictions and offences data.

The following general grounds for exemptions for processing criminal convictions and offences data apply:

- Explicit consent by the data subject
- Protection of a data subject's vital interests
- Processing related to personal data manifestly made public by the data subject
- Processing necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity
- Processing necessary for reasons of substantial public interest
- Processing necessary for scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR, and the conditions referred to in Section 24(b) to (d) of the Implementation Act have been met

Specific exceptions may apply on the basis of Article 33 of the Implementation Act, *eg*, where the processing is carried out by bodies that are responsible pursuant to law for applying criminal law, or where the processing is necessary in order to assess a request from the data subject to take a decision on him or her or to provide a service to him or her.

Child's consent to information society services (Article 8)

The Netherlands did not make use of the option to provide for a lower age limit for the processing of personal data of a child on the basis of Article 8, GDPR.

Automated Decision Making (Article 22)

The Netherlands has made use of the possibility provided by Article 22(2)(b) GDPR, and has implemented exceptions from the prohibition on automated individual decision-making. Article 40 of the Implementation Act sets out that Article 22(1) of the GDPR does not apply if the automated individual decision-making, other than based on profiling, is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out for reasons of public interest. Examples provided by the Explanatory Memorandum to the Implementation Act concern situations where there may be automated individual decision making on the basis of strictly individual characteristics, *eg*, in the case of awarding certain allowances (*eg*, study allowances, child allowances), where there is no reason to require human intervention. In such cases, the controller must take suitable measures to safeguard the data subject's rights, freedoms and legitimate interests. Such suitable measures will in any case have been taken if the right to obtain human intervention, the data subject’s right to express his or her point of view and the right to contest the decision, have been safeguarded.

Processing of national identification number (Article 87)

Article 87 of the GDPR sets out that Member States may further determine the specific conditions for the processing of a national identification number. The Netherlands has made use of this possibility: Article 46 of the Implementation Act sets out that a national identification number may only be processed where explicitly allowed by law, and only for those purposes stipulated by the relevant law.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, the United Kingdom under the GDPR and the LED, the United States (commercial organisations participating in the EU-US Data Privacy Framework), Uruguay, Republic of Korea and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules, standard contractual clauses. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. Explicit informed consent has been obtained;
b. The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. The transfer is necessary for important reasons of public interest;
e. The transfer is necessary for the establishment, exercise or defence of legal claims;
f. The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained;
g. The transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject. Notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State. A transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

After the European Court of Justice Decision of 16 July 2020 (Schrems II), international data transfers to countries that don’t have an equivalent level of protection can take place, if such transfers are based on the 2021 EU Standard Contractual Clauses (SCC). In addition, such in compliance with EDPB guidance, a transfer impact assessment must be conducted in order to assess whether there are reasons to believe that the laws and practices in the third country of destination prevent the recipient from fulfilling its obligations under the SCC.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

An important security measure in line with the GDPR applicable from 1 January 2021 is that, most online payments must be completed with two-step verification. This is an obligation under the Payment Service Directive 2, the European directive for payments by consumers and businesses.

The Netherlands have not implemented any specific regulations on the basis of Articles 24, 25 or 32 of the GDPR. In this respect, the Explanatory Memorandum to the Dutch Implementation Act explains that no general standard will be developed which sets out when an organization has fulfilled its technical and organizational security obligations. However, specific sectoral codes of conduct may be implemented which may contain further concrete standards. For example, in the health sector we see that such security standards already exist (e.g. NEN 7510, which applies as an important information security standard in the health sector).

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

The provisions regarding data breach notifications are mostly identical to Articles 33 and 34 GDPR.

Data breaches that require notification, should be notified to the Dutch DPA by completing an online form through the Dutch DPA website.

The form is available here.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define undertaking and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of undertaking. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called look through liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent
- Data subjects’ rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data
- Certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered material or non-material damage as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of non-material damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

On the basis of Article 58(6) GDPR and in addition to the power to impose fines pursuant to the GDPR, the Dutch DPA has the power to impose an administrative enforcement order (*last onder bestuursdwang*) or an order subject to penalty (*last onder dwangsom*) to enforce obligations laid down by or pursuant to the Implementation Act.

ELECTRONIC MARKETING

The GDPR applies to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted.

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Dutch legislation

Electronic marketing is partially regulated in Article 11.7 of the Dutch Telecommunications Act (Tw). The first paragraph of Article 11.7 of the Tw is the rules for telemarketing that does not involve human intervention. These so-called automatic systems for transmitting commercial, idealistic or charitable communications may only be used if the consumer has given his prior consent. As of 1 July 2021, the Dutch Telecommunications Act changed. As a main rule, also for telemarketing with human intervention, the opt-in system will be used.

New Legislation

The ePrivacy Regulation is a proposed regulation governing the use of electronic communication services within the European Union and is intended to replace the Directive on privacy and electronic communications (Directive 2002/58/EC). In addition to the GDPR, the ePrivacy Regulation represents a core element of EU-level data protection. On 10 February 2021, the Council of the European Union ('the Council') published a new legislative proposal, thereby launching negotiations between the Council, the European Parliament and the European Commission.

In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

ONLINE PRIVACY

Traffic Data

Traffic Data is regulated in Article 11.5 of the Tw. Traffic Data held by a public electronic communications services provider (CSP) must be erased or anonymized when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

- It is being used to provide a value added service; and
- Consent has been given for the retention of the Traffic Data.

Traffic Data can only be processed by a CSP for:

- The management of billing or traffic
- Dealing with customer enquiries
- The prevention of fraud
- The provision of a value added service (subject to consent)
- Market research (subject to consent)

Location Data

(Traffic Data not included) – Location Data is regulated in Article 11.5a of the Tw. Location Data may only be processed:

- If such data is being processed in anonymous form; or
- With informed consent of the individual.

Cookie Compliance

The Netherlands implemented the E-Privacy Directive through the Dutch Telecommunications Act in Article 11.7a. The Authority for Consumers and Markets (ACM) is entrusted with the enforcement of Article 11.7a of the Tw. In addition, in relation to cookie compliance all privacy requirements from the GDPR must be taken into account. The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) has been appointed by law as the supervisory data protection authority and supervises compliance with the GDPR and the Dutch GDPR Implementation Act.

The main rule is that the website operator needs to obtain prior consent from a user before using cookies (opt-in) and needs to clearly and unambiguously inform the user about these cookies (purpose, type of cookie, etc.). Please note that the website operator is not entitled to refuse users access to its website(s) if no consent is given. The requirement to obtain prior consent from a user does not apply in case of functional cookies (e.g. to enable web shopping carts or language choices) and analytical cookies that have little or no impact on the user's privacy (e.g. for testing the effectiveness of certain banners / pages with the aim to improve the website). In such case, the website operator still needs to inform the website visitors about the cookies.

The information collected through cookies are considered personal data, unless the party that places the cookies can prove otherwise.

In case of violation of electronic marketing or online privacy legislation, the ACM can impose fines of up to EUR 900,000 per violation. In some cases, the fine may be even higher and amount to a percentage of the total annual turnover. In case of violation of the GDPR and the Dutch GDPR Implementation Act, the Dutch Data Protection Authority can impose fines up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

KEY CONTACTS

Richard van Schaik
Partner
T +31 20 541 9828
richard.vanschaik@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

NEW ZEALAND

Last modified 18 January 2024

LAW

The Privacy Act 2020 (Act) and its Information Privacy Principles (IPPs) govern how agencies collect, use, disclose, store, retain and give access to personal information. The Act gives the Privacy Commissioner the power to issue codes of practice that modify the operation of the Act in relation to specific industries, agencies, activities or types of personal information. The following codes are currently in place:

- Credit Reporting Privacy Code;
- Health Information Privacy Code;
- Justice Sector Unique Identifier Code;
- Superannuation Schemes Unique Identifier Code;
- Telecommunications Information Privacy Code; and
- Civil Defence National Emergencies (Information Sharing) Code.

The Privacy Commissioner is also currently considering introducing a new code to regulate the collection of biometric information and anticipates that a biometrics code exposure draft will be issued in early 2024. The exposure draft will propose new rules for agencies who want to collect or use biometric personal information. There will be public consultation before the code is finalised.

Enforcement is through the Privacy Commissioner who has the power to investigate any action which appears to interfere with the privacy of an individual and can do so either on a complaint made to the Privacy Commissioner or on the Privacy Commissioner’s own initiative. The Privacy Commissioner can also issue compliance notices requiring agencies to do or refrain from doing something in order to comply with the Act.

Under the Act, an agency can be any person or body of persons, whether corporate or unincorporated, and whether in the public sector or in the private sector.

The Act has an extraterritorial scope — it applies to any actions taken by an overseas organisation in the course of carrying on business in New Zealand, regardless of where the information is or was collected or held and where the person to whom the information relates is located. An organisation may still be treated as carrying on business in New Zealand regardless of whether or not it has a physical place of business in New Zealand, charges any monetary payment for goods or services within New Zealand, or makes a profit from its business in New Zealand. For organisations subject to the Act (whether New Zealand agencies or overseas agencies), it is irrelevant where the personal information was collected, where it is held, or where the individual is or was located (i.e. the Act can extend to personal information collected overseas about foreign data subjects).

In September 2023, the New Zealand government released the Privacy Amendment Bill (Bill), which, if passed, will amend the Privacy Act. The Bill is currently in its first reading however, it is likely to commence into the Select Committee process in 2024. The main amendments to the Act will be the introduction of a new IPP 3A, requiring organisations that

collect personal information 'indirectly' (i.e. not directly from the relevant individual) to provide the individual with information about the processing of their data. Currently, under IPP 3, the Act requires organisations who collect personal information directly from the individual to ensure the individual is aware of certain details, such as the fact of collection, the purposes for which the information will be used, the intended recipients and the individual's right to request access to and correction of their personal information.

IPP 3A will require agencies collecting personal information from a source other than from the individual concerned to take reasonable steps to ensure that the individual is aware of the same information.

The Bill includes certain exceptions to complying with IPP 3A including where the individual has previously been made aware of the organisation's collection of their personal information, or compliance with IPP 3A is not reasonably practicable in the circumstances.

The Bill is set to come into force on 1 June 2025 and the Bill clarifies that IPP 3A will not have retrospective effect.

In September 2023, the Privacy Commissioner issued (non–binding) guidance on the application of the Act's IPPs to the use of AI tools in New Zealand (the Guidance). The Guidance is consistent with key themes from developing international regulations (e.g. the importance of transparency and explainability; accuracy; robustness and security; accountability; and human values and fairness). The Privacy Commissioner has recommended, among other things, that while not mandatory under the Act, it is generally best practice to undertake a Privacy Impact Assessment at the outset of an AI project. The Guidance also recognises an important element which is unique to New Zealand – the need to consider te ao Māori perspectives on privacy (broadly, *te ao Māori* is the Māori worldview including *tikanga Māori - Māori* customs and protocols). Specific concerns identified in the Guidance include:

- bias from systems developed overseas that do not work accurately for Māori;
- collection of Māori information without work to build relationships of trust, leading to inaccurate representation of *Māori taonga* that fail to uphold *tapu and tikanga*; and
- exclusion from processes and decisions of building and adopting AI tools that affect *Māori whānau, hapū, and iwi*, including use of these tools by the public sector.

DEFINITIONS

Definition of personal data

Personal information under the Act is defined as information about an identifiable individual and includes information relating to a death that is maintained by the Registrar General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act.

Definition of sensitive personal data

The Act does not include a concept of 'sensitive personal data', and there is no differentiation between how different types of personal information are to be treated under the Act. However, the Privacy Commissioner has issued (non–binding) guidance defining sensitive personal information as information about the individual that has some real significance to them, is revealing of them, or generally relates to matters that an individual might wish to keep private. This can be contrasted with routine or mundane information that is about a person but is either not particularly revealing or does not reveal information that is very intimate or “private”. The Privacy Commissioner has indicated that information about a person’s race, ethnicity, gender or sexual orientation, sex life, health, disability, age, religious, cultural or political beliefs, activities or memberships will generally be considered sensitive in nature.

Because the Act does not include a concept of sensitive personal data, there are no specific statutory obligations attracting to more sensitive information. However, the Privacy Commissioner's guidance states that agencies have a higher standard of care when they collect or hold sensitive information. While the Act does not specify special procedures for information that is sensitive, the obligations on agencies are stronger with respect to sensitive information and they will be held to a higher standard

of accountability. For example, IPP 5 requires agencies to protect personal information with security safeguards that are reasonable in the circumstances — there will be a higher bar for what is considered reasonable if the information to be protected is sensitive in nature.

Additionally, the codes of practice issued by the Privacy Commissioner may modify the operation of the Act for specific industries, agencies, activities and types of personnel information. The Privacy Commissioner is currently considering introducing a new code to regulate biometric information, which the Privacy Commissioner considers to be particularly sensitive information and requires careful assessment before use.

Definition of agency

Agency is defined under the Act as any person or body of persons, whether corporate or unincorporated, and whether in the public sector (including government departments) or the private sector. Certain bodies are specifically excluded from the definition.

NATIONAL DATA PROTECTION AUTHORITY

The Privacy Commissioner’s Office

Level 13
15 Shortland Street
Auckland 1010
New Zealand

Telephone

+64 9 302 8680
0800 803 909

Email

enquiries@privacy.org.nz

Website

privacy.org.nz

REGISTRATION

There is no obligation on agencies to register or notify the Privacy Commissioner that they are processing personal information.

DATA PROTECTION OFFICERS

The Act requires each agency to appoint one or more individuals to be a privacy officer. The privacy officer may be within or external to the agency (i.e. the privacy officer role may be outsourced to a third party) and does not need to be a New Zealand citizen or reside in New Zealand.

The privacy officer's responsibilities include the following:

- The encouragement of compliance with the personal IPP contained in the Act;
- Dealing with requests made to the agency pursuant to the Act;
- Working with the Privacy Commissioner in relation to investigations relating to the agency; and
- Ensuring compliance with the provisions of the Act.

COLLECTION & PROCESSING

Subject to specific exceptions, agencies may collect, store and process personal information in accordance with the 13 IPPs summarised below.

IPP 1 – Purpose of collection of personal information

An agency must not collect personal information other than for a lawful purpose connected to the agency's functions, and only if the collection of the information is necessary for that purpose.

IPP 2 – Source of personal information

An agency must collect information directly from the relevant individual, unless one of the specified exceptions applies, which include if collection from the individual is not practical in the circumstances, if collection from a third party would not prejudice the interests of the individual, or if the information is publicly available.

IPP 3 – Collection of personal information from subject

Before collecting personal information, an agency has to make the relevant individual aware of certain things, such as the fact that information is being collected, the purposes for which it will be used, and the right to access and request correction of personal information. This is typically done by way of a privacy policy. There are several exceptions where the person collecting information would not need to comply with IPP 3, including where compliance is not reasonably practicable in the circumstances.

IPP 4 – Manner of collection of personal information

Agencies cannot collect personal information by unlawful or unfair means, or in a manner that intrudes to an unreasonable extent upon the personal affairs of the individual concerned. Particular care must be taken when collecting personal information from children or young persons.

IPP 5 – Storage and security of personal information

Agencies must ensure personal information is protected by reasonable security safeguards against loss and unauthorised access, use, modification or disclosure or other misuse. If it is necessary to give personal information to another person (e.g. a service provider), an agency must do everything reasonably within its power to prevent unauthorised use or disclosure of that information.

IPP 6 – Access to personal information

Where an agency holds personal information about an individual, subject to certain exceptions, if requested by the individual, the agency must confirm whether it holds the information and grant the individual access to it. The exceptions include where the information is not readily retrievable or:

- the refusal is for the protection of the health, safety or similar of an individual;
- in an employment context, the information is evaluative (e.g. compiled for the purpose of determining the suitability of an individual for employment) and disclosure would breach an implied promise that was made to the person who supplied the information;
- the information needs protecting because it would involve disclosure of a trade secret or be likely to unreasonably prejudice the commercial position of the person who supplied the information, unless the public interest in disclosure outweighs the withholding of the information;
- the information does not exist or cannot be found;
- the disclosure would involve the unwarranted disclosure of the affairs of another individual;
- the disclosure would breach legal professional privilege; or
- the request is frivolous or vexatious, or the information requested is trivial.

IPP 7 – Correction of personal information

An individual can request an agency to correct information the agency holds about the individual, or attach a statement of a correction sought but not made. If an agency has corrected personal information or attached a statement of a correction sought but not made, if reasonably practicable, it will inform each person or entity to whom it has disclosed that information of that correction or statement. The agency must inform the individual of any action taken as a result of the individuals request.

IPP 8 – Accuracy of personal information to be checked before use or disclosure

Agencies must take reasonable steps to ensure personal information they hold is accurate, up to date, complete, relevant, and not misleading.

IPP 9 – Agency not to keep personal information for longer than necessary

Agencies must not keep personal information for longer than is required for the purposes for which the information may lawfully be used.

IPP 10 – Limits on use of personal information

Agencies must not use personal information obtained in connection with one purpose for any other purpose unless the agency reasonably believes:

- the source of the information is publicly available and it would not be unfair or unreasonable to use that information;
- the use of the information for the other purpose is authorised by the relevant individual;
- non–compliance is necessary to avoid prejudice to the maintenance of the law by any public sector agency:
    - for the enforcement of a law imposing a pecuniary penalty;
    - for the protection of public revenue; or
    - for the conduct of proceedings before a court or tribunal;
- the use of the information for the other purpose is necessary to prevent or lessen a serious threat to public health or safety, or the life or health of an individual;
- the other purpose is directly related to the purpose for which the information was obtained, or the information is used in a form where the individual is not identified, or is used for statistical or research purposes and will not be published in a form where the individual could reasonably be expected to be identified.

IPP 11 – Limits on disclosure of personal information

Agencies must not disclose personal information for any purpose other than the purpose for which it was collected or a purpose directly related to the purpose for which it was collected unless the agency reasonably believes:

- the source of the information is publicly available and it would not be unfair or unreasonable to disclose that information;
- the disclosure is to the relevant individual;
- the disclosure is authorised by the relevant individual;
- non-compliance is necessary:
    - to avoid prejudice to the maintenance of the law by any public sector agency;
    - for the enforcement of a law imposing a pecuniary penalty;
    - for the protection of public revenue; or
    - for the conduct of proceedings before a court or tribunal;
- the disclosure of the information is necessary to prevent or lessen a serious threat to public health or safety, or the life or health of an individual;
- the disclosure is necessary to enable an intelligence and security agency to perform any of its functions;
- the disclosure is necessary to facilitate the sale or other disposition of a business as a going concern; or
- the information is to be used in a form where the individual is not identified, or is used for statistical or research purposes and will not be published in a form where the individual could reasonably be expected to be identified.

IPP 12 – Disclosure to an overseas person

Agencies must not disclose personal information to a foreign person or entity unless the agency reasonably believes:

- the relevant individual authorises the disclosure after being informed by the agency that the foreign person or entity may not be required to protect the information in a way that provides comparable safeguards to those in the Act;
- the foreign person or entity is carrying on business in New Zealand and the agency reasonably believes that, in relation to the information being disclosed, the foreign person or entity is subject to the Act;
- the foreign person or entity is subject to privacy laws that provide comparable safeguards to those in the Act;
- the foreign person or entity is a participant in a prescribed binding scheme;
- the foreign person or entity is subject to privacy laws of a prescribed country; or
- the foreign person or entity is required to protect the information in a way that provides comparable safeguards to those in the Act (for example, pursuant to contractual clauses). New Zealand's Privacy Commissioner has released model contractual clauses that can be used to satisfy these exceptions, but it is not mandatory to use these exact provisions.

IPP 13 – Unique identifiers

Agencies can only assign 'unique identifiers' to an individual if it is necessary to enable the agency to carry out one or more of its functions efficiently. The agency must not assign an individual a unique identifier that it knows has been assigned to that individual by another agency unless the unique identifier is being used for statistical or research purposes only. Additionally, the agency must take reasonable steps to ensure that unique identifiers are only assigned to individuals whose identities are clearly established and that the risk of the unique identifiers being misused is minimised. An agency must not require an individual to disclose any unique identifier assigned to them unless the disclosure is one of the purposes, or directly related to one of the purposes, for which that unique identifier was assigned.

TRANSFER

Generally, an agency should not disclose personal information to another entity unless the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained. Care must be taken that all safety and security precautions are met to ensure the safeguarding of that personal information to make certain that it is not misused or disclosed to any other party.

Transfer of personal information to another agency to hold as the transferring agency's agent (e.g. for safe custody or processing) is not considered a disclosure of the information for the purposes of the Act.

Agencies must not disclose personal information to a foreign person or entity unless the agency reasonably believes:

- the relevant individual authorises the disclosure after being informed by the agency that the foreign person or entity may not be required to protect the information in a way that provides comparable safeguards to those in the Act;
- the foreign person or entity is carrying on business in New Zealand and the agency reasonably believes that, in relation to the information being disclosed, the foreign person or entity is subject to the Act;
- the foreign person or entity is subject to privacy laws that provide comparable safeguards to those in the Act;
- the foreign person or entity is a participant in a prescribed binding scheme;
- the foreign person or entity is subject to privacy laws of a prescribed country; or
- the foreign person or entity is required to protect the information in a way that provides comparable safeguards to those in the Act (e.g. pursuant to contractual clauses). New Zealand's Privacy Commissioner has released model contractual clauses that can be used to satisfy these exceptions, but it is not mandatory to use these exact provisions.

Additionally, the Privacy Commissioner is given the power to prohibit a transfer of personal information from New Zealand to another state, territory, province or other part of a country (State) by issuing a transfer prohibition notice (Notice) if it is satisfied that information has been received in New Zealand from one State and will be transferred by an agency to a third State which does not provide comparable safeguards to the Act and the transfer would be likely to lead to a contravention of the basic principles of national application set out in Part Two of the Organisation for Economic Co–operation and Development (OECD) Guidelines.

In considering whether to issue a Notice, the Privacy Commissioner must have regard to whether the proposed transfer of personal information affects, or would be likely to affect any individual, the desirability of facilitating the free flow of information

between New Zealand and other States, and any existing or developing international guidelines relevant to trans–border data flows.

On December 19, 2012 the European Commission issued a decision formally declaring that New Zealand law provides a standard of data protection that is adequate for the purposes of EU law. This decision means that personal data can flow from the 27 EU member states to New Zealand for processing without any further safeguards being necessary.

Following the decision in the Schrems and Schrems II cases, there have been calls to review New Zealand's adequacy status, primarily due to New Zealand's membership with the Five Eyes network. In January 2024, the European Commission reviewed New Zealand's adequacy status. The review confirmed that New Zealand's adequacy status remains due to New Zealand's strengthened privacy legislation and clarification of certain privacy rules since the adoption of the initial adequacy decision, aligning it further with the EU framework.

SECURITY

An agency that holds personal information shall ensure that the information is kept securely and protected by such security safeguards as are reasonable in the circumstances to protect against loss, access, use, modification, or disclosure that is not authorised by the agency, and other misuse.

If it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency must be done to prevent unauthorised use or unauthorised disclosure of the information.

BREACH NOTIFICATION

Under the Act, any 'privacy breach' which it is reasonable to believe has caused or is likely to cause serious harm to an individual must be notified to the Privacy Commissioner and to the affected individuals.

A 'privacy breach' is any unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, personal information, or any action that prevents the agency from accessing the information on either a temporary or permanent basis.

When assessing whether a privacy breach is likely to cause serious harm, agencies must consider:

- any action taken by the agency to reduce the risk of harm following the breach;
- whether the personal information is sensitive in nature;
- the nature of the harm that may be caused to affected individuals;
- the person or body that has obtained or may obtain personal information as a result of the breach (if known);
- whether the personal information is protected by a security measure; and
- any other relevant matters.

Agencies must notify the Privacy Commissioner and affected individuals as soon as practicable after becoming aware of a notifiable privacy breach. The Privacy Commissioner has issued non-binding guidance that it expects to be notified within 72 hours of an agency discovering a notifiable privacy breach. If it is not reasonably practicable to notify an affected individual or each member of a group of affected individuals, an agency can give a public notice of the breach.

Notification to affected individuals is not required or can be delayed in certain circumstances. For example, notification to affected individuals can be delayed if the agency believes that a delay is necessary because notification or public notice may pose risks for the security of personal information held by the agency and those risks outweigh the benefits of informing affected individuals (for example, if notification of the breach would expose an unremedied security vulnerability).

Anyone who outsources services that involve data processing should be aware that the Act includes an express provision that anything relating to a notifiable privacy breach that is known by an agent is to be treated as being known by the principal agency. This is because the legislators consider that the principal agency should be responsible for informing individuals about a notifiable breach.

ENFORCEMENT

In New Zealand, the Privacy Commissioner is responsible for investigating a breach of privacy laws. The Privacy Commissioner has powers to enquire into any matter if the Privacy Commissioner believes that the privacy of an individual is being, or is likely to be, infringed. The Privacy Commissioner will primarily seek to settle a complaint by conciliation and mediation. If a complaint cannot be settled in this way, a formal investigation may be conducted so that the Privacy Commissioner may form an opinion on how the law applies to the complaint. The Privacy Commissioner’s opinion is not legally binding but is highly persuasive.

If the Privacy Commissioner is of the opinion that there has been an interference with privacy, the Privacy Commissioner may refer the matter to the Director of Human Rights who may then in turn decide to take the complaint to the Human Rights Review Tribunal. The Tribunal will hear the complaint afresh and its decision is legally binding. It can award damages for breaches of privacy.

The Privacy Commissioner can also issue compliance notices requiring agencies to take certain actions, or stop certain activities, in order to comply with the Act. Compliance notices will describe the steps that the Privacy Commissioner considers are required to remedy non–compliance with the Act and will specify a date by which the agency must make the necessary changes. The Privacy Commissioner can also issue access directions requiring agencies to provide individuals access to their personal information.

It is an offence to:

- mislead an agency to access another individual's personal information;
- destroy personal information, knowing that a request has been made to access it;
- without reasonable excuse, obstruct, hinder, or resist the Privacy Commissioner or any other person in the exercise of their powers under the Act;
- without reasonable excuse, refuse or fail to comply with any lawful requirement of the Privacy Commissioner or any other person under the Act;
- give false or misleading statements to the Privacy Commissioner;
- represent directly or indirectly that a person holds any authority under the Act when they do not hold that authority; or
- fail to notify the Privacy Commissioner of a notifiable privacy breach.

The penalty for these offences is a fine of up to NZD 10,000.

ELECTRONIC MARKETING

The Act does not differentiate between the collection of and use of any personal information for electronic marketing or other forms of direct marketing.

The Unsolicited Electronic Messages Act 2007:

- prohibits unsolicited commercial electronic messages (this include email, fax, instant messaging and text messages of a commercial nature – but do not cover Internet pop-ups or voice telemarketing) with a New Zealand link (messages sent to, from or within New Zealand);
- requires consent (which can be express, reasonably inferred, or deemed) from the recipient prior to sending commercial electronic messages;
- requires commercial electronic messages to include accurate information about who authorised the message to be sent;
- requires a functional unsubscribe facility to be included so that the recipient can instruct the sender not to send the recipient further messages; and
- prohibits using address-harvesting software to create address lists for sending unsolicited commercial electronic messages.

The Marketing Association of New Zealand has a code of practice for direct marketing which governs compliance by members of the principles of the code. The code establishes a ‘Do Not Call’ register to which anyone not wanting to receive any direct marketing can register.

ONLINE PRIVACY

Other than compliance with the Act, no additional legislation deals with the collection of location and traffic data by public electronic communications services providers and use of cookies (and similar technologies). The New Zealand Privacy Commissioner has general guidelines on protecting online privacy.

KEY CONTACTS

DLA Piper New Zealand
www.dlapiper.co.nz/

Nick Valentine
Partner
T +64 9 916 3703
nick.valentine@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

NICARAGUA

Last modified 28 January 2024

LAW

Ley No. 787 Ley de Protección de Datos Personales (Law No. 787 Personal Data Protection Law) effective since 29th of March 2012 published in the Official Gazzette No. 61 same day.

DEFINITIONS

Definition of Personal Data

Personal data: It is all the information about a natural or legal person that identifies or makes it identifiable.

Definition of Sensitive Personal Data

Sensitive personal data: It is any information that reveals the racial, ethnic, political affiliation, religious, philosophical or moral, union, health or sexual life, criminal record or administrative, economic and financial misconduct; as well as credit and financial information and any other information that could be grounds for discrimination.

NATIONAL DATA PROTECTION AUTHORITY

Personal Data Protection Directorate (it has not been formally incorporated).

REGISTRATION

Each organisation that collects personal data will have the obligation to register in the Data File Registry.

However, since the Personal Data Protection Directorate has not yet been incorporated, such a Register in practice does not yet exist. Therefore, organisations are unable to materially comply with such registration.

DATA PROTECTION OFFICERS

Any officer responsible for the Data File of each organisation must register in the Data Files Registry that the Personal Data Protection Directorate enables for this purpose.

We must reiterate that this obligation cannot be materially fulfil as the Personal Data Protection Directorate has not been formally incorporated.

COLLECTION & PROCESSING

The law defines data processing as those systematic operations and procedures, automated or not, that allow the collection, registration, recording, conservation, ordering, storage, modification, updating, evaluation, blocking, destruction, deletion, use and cancellation, as well as the transfer of personal data resulting from communications, consultations, interconnections and transfers.

Personal data may only be processed, when they are adequate, proportional and necessary in relation to the scope and specific, explicit and legitimate purposes for which they have been requested.

The purpose of processing the personal data of the user should be to facilitate the improvement, expansion, sale, billing, management, provision of services and acquisition of goods.

TRANSFER

Personal data may be assigned and transferred when the purposes are directly related to the legitimate interest of the assignor and the assignee and with the prior consent of the owner of the data, who must be informed about the purpose of the assignment and identify the assignee.

The consent for the transfer is revocable, by written notification or by any other means that is equated, depending on the circumstances, to the person responsible for the data file.

SECURITY

The necessary technical and organisational measures must be adopted to guarantee the integrity, confidentiality and security of personal data, to avoid its adulteration, loss, consultation, treatment, disclosure, transfer or unauthorised disclosure, and that allow detecting intentional deviations or not, of private information, whether the risks come from human action or the technical means used.

BREACH NOTIFICATION

The legislation does not expressly contemplate the duty of notification of data breach.

Mandatory breach notification

The legislation only contemplates mandatory notification in the event of data breach in the case of Army and Police personnel, and the relevant institutions must be informed immediately.

ENFORCEMENT

Due to the fact that the institution that supervises the application of the norm has not been formally incorporated (Personal Data Protection Directorate), the enforcing of the provisions are not being duly exercised by the government.

ELECTRONIC MARKETING

The data files destined to the sending of advertising, promotions, offers and direct sale of products, goods and services or other analogous activities can only incorporate personal data with the consent of the owner, or when the data appears in publicly accessible sources.

The sending of advertising and promotions, through electronic means, must offer the possibility to the recipient of personal data to express their refusal to continue receiving advertising and promotional content of goods and services or, where appropriate, revoke their consent in a clear and free manner.

Companies or institutions that engage in electronic marketing, advertising and promotional content must be protected by means of a contract that establishes that the personal data contained in a data file has been obtained with the unequivocal and informed consent of the owners or that it has been obtained from publicly accessible sources.

ONLINE PRIVACY

The normative states that when the officer of the data file uses mechanisms in remote or local means of electronic, optical or other technology communication (cookies), which allow to collect personal data automatically and simultaneously, while the data owner makes contact with them. At that time, the owner must be informed about the use of these technologies, that personal data is obtained through them and the way in which they can be disabled.

The location data is not regulated.

KEY CONTACTS

Central Law
central-law.com/

Álvaro Molina Vaca
Partner
Central Law
T +505 2278 6045
amolina@central-law.com

Avil Ramírez Mayorga
Associate
Central Law
T +505 2278 6045
aramirezm@central-law.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

NIGER

Last modified 8 January 2024

LAW

The data protection regime in Niger is governed by the following laws and regulations:

- Law n° 2023-31 of 04 July 2023 amending law n°2022-59 of 16 December 2022 on the protection of personal data;
- Law n°2022-59 of December 16, 2022 relating to the protection of personal data;
- Decree No. 2020-309/PRN/MJ of April 30, 2020 setting the terms of application of Law No. 2017-28 of May 3, 2017 on the protection of personal data as amended and supplemented by Law No. 2019-71 of December 24, 2019;
- Order No. 000045 of October 5, 2020 determining the profile and setting the conditions of remuneration of the personal data protection correspondent;
- Law No.2018-45 of July 12, 2018 on the regulation of electronic communications in Niger; and
- Cybercrime Amendment Act 2022 (2019).

DEFINITIONS

Definition of Personal Data

Any information of any nature related to an identified or identifiable natural person, including sounds and images, directly or indirectly referencing an identification number, or one or more elements specific to his physical, physiological, genetic, psychological, cultural, social, or economic identity (Article 1 of the Law).

Definition of Sensitive Personal Data

Any personal data relating to religious or philosophical opinions or activities, political affiliation, sex life, race, health, social measures, prosecutions, and criminal or administrative sanctions (Article 1 of the Law).

NATIONAL DATA PROTECTION AUTHORITY

High Authority for the Protection of Personal Data (known by its French Acronym “**HAPDP**”).

The HAPDP is composed under the new Article 7 of the 2023 Act amending the 2022 Act on personal data of eleven members chosen because of their legal and / or technical competence.

In accordance with the new Article 6 of the aforementioned law, The HAPDP is attached to the Presidency of the Republic. The HAPDP is an independent administrative authority The HAPDP's role is to ensure that any processing of personal data is in accordance with the Law. In addition, the HAPDP's responsibilities include informing data controllers and data subjects of their rights and obligations, handling complaints, conducting audits, and sanctioning data controllers who are in breach of the Law.

REGISTRATION

The registration of processing activities via a "*register of processing activities&#8221*; does not exist in Niger.

The processing of personal data is subject to prior notification to the HAPD. If a data controller appoints a data protection officer, notification is unnecessary unless personal data is being transferred across national borders. Additionally, Article 64 Law n° 2022-59 of December 16, 2022 relating to the protection of personal data provides that the data controller must create an annual report for the HAPDP regarding personal data which is stored within the period, as fixed by the HAPDP, in relation to the purposes for which each type of processing activity was carried out.

DATA PROTECTION OFFICERS

There is no provision in the law relating to the appointment of a data protection officer.

However, Article 79 of the Law n°2022-59 of December 16, 2022 relating to the protection of personal data pertains to the designation of the personal data protection correspondent, which is defined in Article 1 as the person designated by the company carrying out the processing of personal data, to whom data subjects or interested persons may address any queries.

Article 79 of the of the aforementioned Law continues to state that the correspondent must possess the required qualifications to carry out their duties and be able to make a list of processing activities immediately accessible for any person requesting the same. The correspondent is exempt from any sanction on the part of the employer resulting from the carrying out of their duties.

Furthermore, the data controller's designation of a correspondent must be notified to the HAPDP and, in the event of failures to carry out their duties, may be discharged by request, or after consultation, from the HAPDP.

COLLECTION & PROCESSING

Any processing of personal data can only take place if the person concerned, the data subject, has expressed his consent in a free, specific, informed, and unambiguous manner. The processing of personal data is considered legitimate if the data subject gives his / her prior express consent.

The requirement of prior consent may be waived where the controller is duly authorised and the processing is necessary for:

- the performance of a contract to which the data subject is party or in order to take pre-contractual measures at his request;
- complying with a legal obligation to which the controller is subject to;
- protecting the interests or fundamental rights and freedoms of the data subject; and
- the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.

The collection and processing of personal data must comply with the following principles:

- **The principles of lawfulness, fairness and transparency:** Data must be processed fairly, lawfully, and transparently. The lawfulness of the processing refers to its legal basis (legal obligation, contractual obligation, etc.). Fairness of processing refers to the manner in which the data are collected. This principle refers to the individual's right to information. Data must not have been collected and must not be processed without the knowledge of the data subject. This principle also requires providing data subjects with several pieces of information (on the processing of their data, but also on their rights).
- **The principle of proportionality:** Data must be adequate, relevant, and not excessive in relation to the purposes for which they are collected and further processed. The data controller must not collect more data than it actually needs. Thus, only data strictly necessary for the achievement of the specified purpose must be collected.
- **The principle of accuracy:** The data must also be accurate and, where necessary, updated. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they are collected and further processed, are erased or rectified.

The obligations of the Data controller include among other things:

- data is collected and processed fairly and lawfully;

- data is collected for specified, explicit and legitimate purposes and subsequently processed in a manner that is compatible with such purposes;
- data is adequate, relevant and not excessive in relation to the purposes for which it was collected;
- collected data is accurate, complete;
- collected data is retained in a form that allows the identification of the data subjects for a period that is no longer than necessary for the purposes for which it was collected;
- data subjects are informed of the data processing;
- data subjects have given their consents to the data processing;
- data subjects have the right to access the data and request amendments or deletions;
- persons with access to the system can only access the data they are allowed to;
- non-authorised persons cannot read, copy, modify, destroy, or move data;
- all data introduced in the system is authorised;
- non-authorised persons will not use data transmission facilities to enter into the data processing system;
- the identities of third parties having access to personal data will be checked;
- data is backed up with security copies; and
- data is renewed and converted to preserve it.

Under the 2022 Personal Data Act, the processing of personal data is subject to a prior notification to the HAPDP. The notification must include an undertaking that the processing meets the requirements of the Law.

However, for certain types of personal data processing, the prior authorisation of the HAPDP is required. This is particularly the case for the processing of personal data relating to genetic, medical data, and scientific research.

By contrast, the Data subject is entitled to an number of rights of which some are listed below:

Right of information: Pursuant to Article 68 of the 2022 Personal Data Act , the data controller must inform the data subject of:

- the identity and, where applicable, that of its duly authorised representative;
- the specific purposes of the processing for which the data is intended;
- the categories of data concerned;
- the recipient(s) to whom the data may be communicated;
- the possibility of refusing to appear on the file;
- the existence of a right of access to data concerning the person and a right to rectify this data; and
- the possibility of any data transfer to a third party.

Right of access: Pursuant to Article 69 of the Personal Data Act 2022, the data subjects can obtain from the data controller the following:

- information allowing to know and dispute the processing of personal data;
- confirmation of whether his / her personal data forms part of the processing;
- a copy of the data subject's personal data, as well as any available information on the data's origin; and
- information relating to the purposes of the processing, the categories of personal data processed and the recipients or categories of recipients to whom the data are communicated.

Right to rectification: Under the provisions of Article 71 of the 2022 Personal Data Act , any natural person who can prove his or her identity may require the data controller to rectify, complete, update, block, or delete, as the case may be, any personal data concerning him or her that is inaccurate, incomplete, ambiguous, out of date, or whose collection, use, communication, or storage is prohibited.

Right to erasure: Under the provisions of Article 73 of the 2022 Personal Data Act, the data subject shall have the right to obtain from the controller the erasure of personal data relating to him or her and the cessation of the dissemination of such data, in particular with regard to personal data which the data subject made available when he / she was a minor, or for one of the following reasons:

- the data is no longer necessary for the purposes for which they were collected or processed;
- the data subject has withdrawn the consent on which the processing is based or where the authorised retention period has expired and there are no other legal grounds for processing the data;
- the data subject objects to the processing of personal data relating to him or her where there is no legal ground for such processing;
- the data processing does not comply with the provisions of this Law; or
- for any other legitimate reason.

Right to object: Any data subject has the right to:

- oppose the processing of their personal data;
- oppose the processing of their personal data for prospecting purposes; and
- be informed before his / her personal data is communicated to third parties.

Interconnection of personal data shall:

- not discriminate against or limit the fundamental rights, freedoms, and guarantees of data holders;
- ensure the use of appropriate safety measures; and
- take into account the principle of relevance.

TRANSFER

Transfer of personal data to another country is allowed only when that country provides a superior or equivalent level of protection for privacy, freedoms and fundamental rights of individuals regarding the processing of personal data (Article 62 of the Law).

SECURITY

Article 82 of the 2022 Data Protection Act sets out the security obligations of data controllers and processors with regard to the protection of personal data. They must put in place technical and organisational measures to prevent distortion, damage or unauthorised access to such data, taking into account the nature, scope, context and purposes of the processing, as well as the risks to individuals. These measures may include pseudonymisation, encryption, anonymisation and encryption of personal data, as well as regular testing, analysis and evaluation procedures to ensure the security of the processing. Appropriate security policies must also be put in place, including the obligation of protection by design and protection by default of personal data necessary for each specific purpose of processing.

BREACH NOTIFICATION

Under article 83 of the 2022 Personal Data Protection Act, the controller of personal data is required to notify the Data Protection Authority (HAPDP) of any personal data breach as soon as it becomes aware of it. This notification must be made without delay and, in the event of a high risk to the rights and freedoms of the data subjects, the data controller must also inform the data subjects as soon as possible. However, the controller is not required to notify a data breach if it is reasonable to believe that the breach does not present a risk to the rights and freedoms of the data subjects. It is important to note that failure to comply with this notification obligation must be justified and substantiated by the data controller to the data protection authority. Failure to comply with this obligation may result in criminal penalties, such as imprisonment and fines, as set out in Article 98 of the Act.

Mandatory Breach Notification

Mandatory notification of personal data breaches is provided for in Article 83 of the 2022 Personal Data Protection Act. According to this article, as soon as the data controller becomes aware of a personal data breach, it must inform the HAPDP without delay. In addition, if the breach is likely to result in a high risk to the rights and freedoms of an individual, the controller must notify the data subject of the security breach as soon as possible.

ENFORCEMENT

The law empowers the HAPDP to impose various sanctions depending on the severity of the infringement. However, the level of enforcement remains quite low due to resource limitations and the fact that this field of law is still new to the administration and business and data subjects.

The HAPDP may, directly or through an expert authorized for this purpose, carry out checks and controls on any processing of personal data. In fulfilment of their duties, the HAPDP officers have access to places, premises, enclosures, installations or establishments used for the processing of personal data and which are for professional use, with the exception of those parts of the premises used for private purposes.

On completion of its checks and inspections, the HAPDP may impose the following administrative sanctions on offenders, without prejudice to criminal prosecution:

- a warning;
- formal notice;
- injunction to cease data processing;
- blocking of certain personal data;
- lump-sum fines;
- withdrawal of authorization.

The amount of the fine is proportionate to the seriousness of the breaches committed and to the benefits derived from the breach. The fine may not exceed the sum of XOF 100,000,000.

In the event of a repeat offence within two years of the date on which the financial penalty previously imposed became final, the amount may not exceed XOF 200,000,000 or, in the case of a company, 5% of the turnover excluding tax for the last financial year for which the accounts have been closed, subject to a limit of XOF 500,000,000.

Unlawful processing of sensitive data, direct canvassing without prior consent, failure to comply with security measures, misuse, fraudulent, unfair or unlawful collection of data, unauthorised communication of personal data, obstructing the exercise of the rights of the person concerned, unlawful storage and unauthorised disclosure of personal data are punishable by imprisonment and a fine.

Depending on the nature of the offence, the penalty may range from three (3) months to five (5) years' imprisonment and a fine of up to 50,000,000 francs.

Sanction by the data protection Authorities may be appealed before the competent administrative court.

ELECTRONIC MARKETING

The personal data Act will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name).

The general rule for electronic marketing is that it requires the express consent of the recipient (see Article 58 of Law No.2018-45 of July 12, 2018 on the regulation of electronic communications in Niger).

Even when a marketer has the consent of a data subject, that consent can be withdrawn by the data subject under Article 28 of the Personal Data Act.

The data subject has the right to object at any time to the use of his/her personal data for such marketing.

This right to object must be explicitly brought to the attention of the data controller.

However, the data controller may not respond favorably to a request to exercise the right to object if it demonstrates the existence of legitimate reasons justifying the processing, which override the interests, fundamental rights and freedoms of the data subject.

ONLINE PRIVACY

The Law does not provide any specific rules for governing cookies and location data.

However, pursuant to Article 82 of the 2022 Data Protection Act, data controller must implement all appropriate technical and organizational measures to preserve the security and confidentiality of the data, including protecting the data against accidental or unlawful destruction, accidental loss, alteration, distribution or access by unauthorized persons.

KEY CONTACTS

Geni & Kebe
www.dlapiperafrica.com/senegal

Dr. Sangare Mouhamoud
Associate
Geni & Kebe
T +225077910754l
m.sangare@gsklaw.sn

Dr. Francky Lukanda
Senior Associate
Geni & Kebe
T +2250584344660
f.lukanda@gsklaw.sn

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

NIGERIA

Last modified 18 January 2024

LAW

Principal regulation

Data Protection Act

The Act has been enacted to safeguard the fundamental rights and freedoms, and the interests of data subjects, as guaranteed under the Constitution of the Federal Republic of Nigeria. Among other things, the objective of the Act include: the protection of personal information; establishing the Nigeria Data Protection commission for the regulation of the processing of personal information; promoting data processing practices that safeguard the security of personal data and privacy of data subjects; protect data subjects’ rights, and provide means of recourse and remedies, in the event of the breach of the data subject’s rights; and strengthening the legal foundations of the national digital economy and guarantee the participation of Nigeria in the regional and global economies through the beneficial and trusted use of personal data etc. The Data Protection Act received Presidential assent on 13 June 2023.

Subsidiary legislation

Nigeria Data Protection Regulation

The personal and territorial scope of the NDPR is defined by citizenship and physical presence. It applies to residents of Nigeria, as well as Nigerian citizens abroad. The NDPR provides legal safeguards for the processing of personal data. Under the NDPR, Personal Data must be processed in accordance with a specific, legitimate and lawful purpose consented to by the Data Subject.

Implementation Framework for the Nigeria Data Protection Regulation

The Framework builds on the NDPR to ensure a tailored implementation of the data protection regime in Nigeria. It serves as a guide to data controllers and administrators / processors to understand the standards required for compliance within their organisations. The Framework is to be read in conjunction with the NDPR and does not supersede the NDPR.

Guidelines for the Management of Personal Data by Public Institutions in Nigeria

The Guidelines apply to all public institutions (PIs) in Nigeria, including ministries, departments, agencies, institutions, public corporations, publicly funded ventures, and incorporated entities with government shareholding, either at the Federal, State or Local levels, that process the personal data of a data subject. The Guidelines mandate all PIs to protect personal data in any incidence of processing of such data. Processing in this context retains the same meaning it has under the NDPR. All forms of personal data of a Nigerian citizen, resident or non-Nigerian individual that has interactions with PIs, or such PIs have access to the personal data in furtherance of a statutory or administrative purpose, are to be protected in accordance with the NDPR or any other law or regulation in force in Nigeria.

Sectoral laws

In addition to the principal legislation mentioned, the Constitution of the Federal Republic of Nigeria and various sector-specific laws make different provisions for privacy and data protection matters. Key provisions in the mentioned laws are outlined hereunder:

The laws

Constitution of the Federal Republic of Nigeria 1999 (As Amended)

The Nigerian Constitution provides Nigerian citizens with a fundamental right to privacy. Section 37 of the Constitution guarantees privacy protections to citizens in their homes, correspondence, telephone conversations and telegraphic communications. The Constitution does not define the scope of “privacy” or contain detailed privacy provisions.

Child Rights Act 2003

The Child Rights Act 2003 reiterates the constitutional right to privacy as relates to children. Section 8 of the Act guarantees a child’s right to privacy subject to parent or guardian rights to exercise supervision and control of their child’s conduct. Some Nigerian states have also enacted Child Rights Laws. Under the Act / Laws, age of a child is any person under the age of 18.

Consumer Code of Practice Regulations 2007 (NCC Regulations)

The Nigerian Communications Commission (NCC) issued the NCC Regulations which requires all licensees to take reasonable steps to protect customer information against improper or accidental disclosure, and ensure that such information is securely stored and not kept longer than necessary. The NCC Regulations further prohibit the transfer of customer information to any party except to the extent agreed with the customer, as permitted or required by the NCC or other applicable laws or regulations.

Consumer Protection Framework 2016 (Framework)

The Consumer Protection Framework 2016 was enacted pursuant to the Central Bank of Nigeria Act 2007. The Framework includes provisions that prohibit financial institutions from disclosing customers’ personal information. The Framework further requires that financial institutions have appropriate data protection measures and staff training programs in place to prevent unauthorized access, alteration, disclosure, accidental loss or destruction of customer data. Financial services providers must obtain written consent from consumers before personal data is shared with a third party or used for promotional offers.

Credit Reporting Act 2017

The Credit Reporting Act establishes a legal and regulatory framework for credit reporting by Credit Bureaus. Section 5 of the Act requires Credit Bureaus to maintain credit information for at least 6 years from the date that such information is obtained, after which the information must be archived for a 10-year period prior to its destruction. Section 9 of the Act provides the rights of data subjects (i.e. persons whose credit data are held by a Credit Bureau) to privacy, confidentiality and protection of their credit information. Section 9 further prescribes conditions under which the credit information of the data subject may be disclosed.

Cybercrimes (Prohibition, Prevention Etc) Act 2015

The Cybercrimes (Prohibition, Prevention Etc) Act provides a legal and regulatory framework that prohibits, prevents, detects, prosecutes and punishes cybercrimes in Nigeria. The Act requires financial institutions to retain and protect data and criminalizes the interception of electronic communications.

Freedom of Information Act, 2011 (FOI Act)

The FOI Act seeks to protect personal privacy. Section 14 of the FOI Act provides that a public institution is obliged to deny an application for information that contains personal information unless the individual involved consents to the disclosure, or where

such information is publicly available. Section 16 of the FOI Act provides that a public institution may deny an application for disclosure of information that is subject to various forms of professional privilege conferred by law (such as lawyer-client privilege, health workers-client privilege, etc.).

National Identity Management Commission (NIMC) Act 2007

The NIMC Act creates the National Identity Management Commission (NIMC) to establish and manage a National Identity Management System (NIMS). The NIMC is responsible for enrolling citizens and legal residents, creating and operating a National Identity Database and issuing Unique National Identification Numbers to qualified citizens and legal residents. Section 26 of the NIMC Act provides that no person or corporate body shall have access to data or information in the Database with respect to a registered individual without authorization from the NIMC. The NIMC is empowered to provide a third party with information recorded in an individual’s Database entry without the individual’s consent, provided it is in the interest of National Security.

National Health (NH) Act 2014

The NH Act provides rights and obligations for health users and healthcare personnel. Under the NH Act, health establishments are required to maintain health records for every user of health services and maintain the confidentiality of such records. The NH Act further imposes restrictions on the disclosure of user information, and requires persons in charge of health establishments to set up control measures for preventing unauthorized access to information. The NH Act applies to all information relating to patient health status, treatment, admittance into a health establishment, and further applies to DNA samples collected by a health establishment.

Nigerian Communications Commission (registration of telephone subscribers) Regulation 2011

Section 9 and 10 of the Nigerian Communications Commission Regulation provides confidentiality for telephone subscribers

records maintained in the NCC’s central database. The Regulation further provides telephone subscribers with a right to view and update personal information held in the NCC’s central database of a telecommunication company in camera.

DEFINITIONS

Definition of personal data

Personal Data is defined as any information relating to an individual, who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual. Personal data is a broad term, encompassing anything from a name, address, photo, email address, bank details, social networking website posts, medical information, and other unique identifier such as, but not limited to, MAC address, IP address, IMEI number, IMSI number, SIM and others.

Definition of personal data breach

Personal Data Breach is defined as a breach of security of a data controller or data processor leading to or likely to lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Definition of data subject

Data Subject means a person to whom personal data relates.

Definition of data controller

Data Controller means a person, private entity, public commission, agency or any other body who, either alone, jointly or in common with other persons, or as a statutory body, determines the purposes for and manner in which Personal Data is processed or is to be processed.

Definition of personal data breach

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Definition of processing

Processing means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Definition of Sensitive Personal Data

Sensitive Personal Data means personal data relating to any of the following:

- genetic and biometric data, for the purpose of uniquely identifying a natural person;
- race or ethnic origin;
- religious or similar beliefs, such as those reflecting conscience or philosophy;
- health status;
- sex life;
- political opinions or affiliations; and
- trade union memberships.

NATIONAL DATA PROTECTION AUTHORITY

Nigeria Data Protection Commission

The Nigeria Data Protection Commission (the Commission) was established under the Nigeria Data Protection Act 2023 (the Act) as the supervisory and regulatory authority for data protection in Nigeria, a function previously undertaken by the Nigeria Data Protection Bureau (NDPB). Essentially, the Commission is the successor-in-title to the duties, power and functions of the NDPB.

REGISTRATION

Data controllers and data processors of major importance must register with the Commission within six months after the commencement of the Act or of becoming a data controller or data processor of major importance. Data controller or data processor of major importance is defined under the Act to mean a data controller or data processor that is resident or operating in Nigeria and processes the personal data of more than such number of data subjects who are within Nigeria as the Commission may prescribe, or such other class of data controller or data processor processing personal data of particular value or significance to the economy, society or security of Nigeria, as the Commission may designate. The Act even though it defines data controllers and data processors of major importance it does not define the measure of processing that would classify a controller or processor as being of major importance. It is likely that regulations issued by the Commission in the future will address this.

DATA PROTECTION OFFICERS

The Nigerian Data Protection Act 2023 requires Data Controllers to designate a Data Protection Officer (**DPO**) who will be responsible for ensuring internal compliance with the Act, other applicable data protection directives, and serving as a point of contact between the Data Controller and the regulatory body (Nigeria Data Protection Commission). The Data Protection Officer may be an employee of a Data Controller or engaged by a service contract.

COLLECTION & PROCESSING

Collection

Personal Data must be collected and processed in accordance with a specific, legitimate and lawful purpose consented to by the Data Subject:

- Prior to Personal Data collection, Controllers must provide Data Subjects with relevant information, including the identity and contact details of the Controller, contact details of its Data Protection Officer and the intended purpose and legal basis for Personal Data processing;
- The legitimate interests pursued by the Controller or third party must be stated;
- The recipients or categories of recipients of the Personal Data, if any;
- Where applicable, the fact that the Controller intends to transfer Personal Data to a third country or international organization, and the existence or absence of an adequacy decision by the Agency, the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
- Data subjects must be provided with notice of their right to:
    a. request access to and rectification of Personal Data maintained by the Controller;
    b. withdraw consent for further processing by the Controller at any time; and
    c. lodge a complaint with the relevant authority; and
- Where the Controller intends to process Personal Data for a purpose other than for which it was collected, the Controller must provide Data Subjects with any relevant information on the additional purpose prior to further processing.

Processing

Personal Data Processing is lawful if at least one of the following applies:

- The data subject has given consent to the processing of his or her Personal Data for one or more specific purposes and the data is processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach;
- Processing is necessary for compliance with a legal obligation to which the Controller is subject under;
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- Processing is necessary for the performance of a contract to which the Data Subject is party to or in order to take steps at the request of the Data Subject prior to entering into a contract; and / or
- Data processing by a third party is governed by a written contract between the third party and the authorised Data Controller. Accordingly, any person engaging a third party to process the data obtained from Data Subjects shall ensure compliance with the Nigerian Data Protection Act 2023.

TRANSFER

The Data Protection Act on transfer of personal data has provided that such transfer is permissible if the recipient of the data is subject to a law, binding corporate rules, contractual clauses, code of conduct or certification mechanism that affords an adequate level of protection with respect to the personal data.

To ensure the level of adequacy required by the recipient country of personal data, the following will occur:

- a data controller or processor shall record the basis for transfer and adequacy of protection in that country;

- the Commission may make regulations requiring data controllers and processors to notify it of the measures in place to explain their adequacy in accordance with the Act;
- the Commission may by regulation designate categories of personal data that are subject to additional specified restrictions on transfer to another country based on the nature of such personal data and risks to data subjects.

Other forms of assessment to be taken into account to ensure adequacy of protection include:

- availability of enforceable data subject rights, the ability of a data subject to enforce such rights through administrative or judicial redress, and the rule of law;
- existence of any appropriate instrument between the Commission and a competent authority in the recipient jurisdiction that ensures adequate data protection;
- access of a public authority to personal data;
- existence of an effective data protection law;
- existence and functioning of an independent, competent data protection, or similar supervisory authority with adequate enforcement powers; and
- international commitments and conventions binding on the relevant country and its membership of any multilateral or regional organisations.

The Commission shall issue guidelines for these assessments in line with the factors that have been outlined above. The Commission may determine if a country, region or specified sector within a country has the adequate level of protection. The Commission may approve binding corporate rules, codes of conduct, certification mechanisms or similar instruments for data transfer proposed to it if it meets the standards specified in this Act.

In the absence of adequacy of protection as specified by the Act, transfer of personal data from Nigeria to another country is possible if at least one of the following conditions are met:

- The data subject has provided and not withdrawn consent to such transfer after having been informed of the possible risks of such transfers for the data subject due to the absence of adequate protections;
- transfer is necessary for the performance of a contract to which a data subject is a party or in order to take steps at the request of a data subject, prior to entering into a contract;
- transfer is for the sole benefit of a data subject and it is not reasonably practicable to obtain the consent of the data subject to that transfer or if it were reasonably practicable to obtain such consent, the data subject would likely give it;
- transfer is necessary for important reasons of public interest;
- transfer is necessary for the establishment, exercise, or defense of legal claims; or
- transfer is necessary to protect the vital interests of a data subject or of other persons, where a data subject is physically or legally incapable of giving consent.

SECURITY

Anyone involved in data processing or the control of data has the responsibility to develop security measures to protect data. Such measures include but are not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption technologies, developing organizational policies for handling Personal Data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff.

BREACH NOTIFICATION

There is an obligation on a data processor, on becoming aware of a breach to do the following:

- notify the data controller or processor that engaged it, describing the nature of the personal data breach including where possible, the categories and approximate number of data subject and records concerned;
- respond to all information requests from the data controller or processor that engaged it;
- within 72 (seventy two) hours of becoming aware of a breach, if the breach is likely to result in a risk to the rights and freedoms of individuals, the data controller is obligated to notify the Commission. The data controller will immediately

communicate the breach in plain and clear language including advice about measures the data subject could take to mitigate the effect of the breach. In the event that it is not feasible, a public communication in one or more widely used media sources in which the data subject will likely be informed, can be used.

ENFORCEMENT

The Commission is saddled with supervisory and enforcement responsibilities in respect of data protection matters in Nigeria. It collaborates with security agencies like the office of the Inspector General of Police to ensure full compliance and enforcement. Where the Commission is satisfied that a data controller or data processor has violated or is likely to violate any requirement under the Act or any subsidiary legislation, the Commission may make an appropriate compliance order against that data controller or data processor. The order made by the Commission may include:

- warning that certain act or omission is likely to be a violation of one or more provisions under the Act or any subsidiary legislation or orders issued under it;
- requirement that the data controller or data processor complies with such provisions, including complying with the requests of a data subject to exercise one or more rights under the Act; or
- cease and desist order requiring the data controller or data processor to stop or refrain from doing an act, which is in violation of the Act, including stopping or refraining from processing personal data that is the subject of the order.

If the Commission, after completing an investigation, is satisfied that a data controller or data processor has violated any provision of the Act it:

- may make any appropriate enforcement order or impose a sanction on the data controller or data processor; and
- shall inform the data controller or data processor, and if applicable, any data subject who lodged a complaint leading to the investigation, in writing of its decision.

An enforcement order made or sanction imposed shall include:

- requiring the data controller or data processor to remedy the violation;
- ordering the data controller or data processor to pay compensation to a data subject, who has suffered injury, loss, or harm as a result of a violation;
- ordering the data controller or data processor to account for the profits realised from the violation; or
- ordering the data controller or data processor to pay a penalty or remedial fee.

Applicable remedial fees are as follows:

- For data controllers / processors of major importance, the organization can be fined up to 2% of its annual revenue or 10 million Naira, whichever is greater;
- In case of a data controller / processors not of major importance, the organization can be fined up to 1% of its annual revenue or 2 million Naira, whichever is greater.

Also, a data controller or data processor, who fails to comply with orders made by the Commission commits an offence and is liable on conviction to — (a) a fine of up to the — (i) higher maximum amount, in the case of a data controller or data processor of major importance, or (ii) standard maximum amount, in the case of a data controller or data processor not of major importance; or (b) imprisonment for a term not more than one year or both.

ELECTRONIC MARKETING

The NCC Regulations provide that no licensee shall engage in unsolicited telemarketing unless it discloses:

- At the beginning of the communication, the identity of the licensee or other person on whose behalf it is made and the precise purpose of the communication. During the communication, the full price of any product or service that is the subject of the communication must be specified.
- The person receiving the communication shall have an absolute right to cancel the agreement for purchase, lease or other supply of any product or service within seven (7) days of the communication, by calling a specific telephone number

(without any charge, and that the Licensee shall specifically identify during the communication) unless the product or service has by that time been supplied to and used by the person receiving the communication.

Licensees are required to conduct telemarketing in accordance with any “call” or “do not call’ preferences recorded by the consumer, at the time of entering into a contract for services or after, and in accordance with any other rules or guidelines issued by the Commission or any other competent authority.

Internet Service Providers (ISP)

The NCC Legal Guidelines for Internet Service Providers (ISP) provides that Commercial Communications ISPs must take reasonable steps to promote compliance with the following requirements for commercial email or other commercial communications transmitted using the ISP’s services:

- The communication must be clearly identified as a commercial communication.
- The person or entity on whose behalf the communication is being sent must be clearly identified.
- The conditions to be fulfilled in order to qualify for any promotional offers, including discounts, rebates or gifts, must be clearly stated.

Promotional contests or games must be identified as such, and the rules and conditions to participate must be clearly stated. Persons transmitting unsolicited commercial communications must take account of any written requests from recipients to be removed from mailing lists, including by means of public “opt-out registers” in which people who wish to avoid unsolicited commercial communications are identified.

Advertising

The Advertising Regulatory Council of Nigeria Act 2022 (ARCON Act) is the apex law regarding advertising and marketing communications in Nigeria; its scope covers both terrestrial and online advertisements. The Nigerian Code of Advertising Practice Sales Promotion and Other Rights / Restrictions on Practice (5th Edition) which continues in force under the ARCON Act, provides that all advertisements and marketing communications directed at the Nigerian market using the Internet or other electronic media must comply with the following requirements:

- The commercial nature of such communications must not be concealed or misleading, it should be made clear in the subject header.
- Terms of the offer should be clear and devices should not be used to conceal or obscure any material factors, such as price or other sales conditions likely to influence customer decisions.
- The procedure for concluding a contract should be clear.
- Due recognition must be given to the standards of acceptable commercial behavior held by public groups before posting marketing communications to such groups using electronic media.
- Unsolicited messages should not be sent except where there are reasonable grounds to believe that consumers who receive such communications are interested in the subject matter or offer.
- All marketing communications sent via electronic media should include a clear and transparent mechanism enabling consumers to expressly opt-out from future solicitations.
- Care should be taken to ensure that neither the marketing communication, or applications used to enable consumers to open marketing or advertising messages, interfere with consumers normal use of electronic media.
- Customer information must not be transferred to any party except to the extent agreed with the Customer, as permitted or required by the NCC or other applicable laws or regulations.

ONLINE PRIVACY

The Constitutional right to privacy applies to electronic media, including mobile devices and the Internet. Violations of these rights as safeguarded by the constitution may be subject to civil enforcement under the Fundamental Rights Enforcement Procedure Rules, 2009.

According to the Nigeria Data Protection Act, data controllers are obligated to perform a data privacy impact assessment where processing personal data could potentially pose a substantial risk to the rights and freedoms of a data subject, taking into

consideration the nature, scope, context and purposes of such processing. Where the probability of high risks is established by the impact assessment, the controller is obligated to consult the Commission before processing.

The Nigeria Data Protection Regulations requires all mediums through which Personal Data is collected or processed to display a simple and conspicuous privacy policy, easily understood by the targeted Data Subject class. The privacy policy must contain the following, in addition to any other relevant information:

- What constitutes Data Subject consent;
- Description of Personal Data to be collected;
- Purpose of Personal Data collection;
- Technical methods used to collect and store personal information (i.e. cookies, web tokens etc.);
- Access (if any) of third parties to Personal Data and purpose of access;
- An overview of data processing principles under the NDPR;
- Available remedies for privacy policy violation;
- Timeframes associated with available remedies; and
- Any limitation clause, provided that no limitation clause shall avail any Data controller who acts in breach of the principles of lawful processing set out in the NDPR.

KEY CONTACTS

Olajide Oyewole LLP
www.olajideoyewole.com/

Sandra Oyewole
Partner
Olajide Oyewole LLP
T +234 1 279 3674
soyewole@olajideoyewole.com

Adewumi Salami
Associate
Olajide Oyewole LLP
T +234 1 279 3674
asalami@olajideoyewole.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

NORTH MACEDONIA

Last modified 17 January 2024

LAW

The Republic of North Macedonia regulates personal data protection issues with the Law on Personal Data Protection (Official Gazette of the Republic of North Macedonia, no. 42/20 and 294/21, “**DP Law**”), effective 24 February 2020. Data controllers and data processors had an 18-month period from the DP Law’s entry into force (i.e. until 24 August 2021) to harmonize their operations with the DP Law. This period has been informally prolonged for additional six months, during which time the data protection authority assisted companies in the implementation of the new rules through education and corrective measures, as opposed to directly issuing fines for non-compliance.

The DP Law is largely harmonized with the General Data Protection Regulation (GDPR) of the European Union (EU).

DEFINITIONS

Definition of personal data

The DP Law defines personal data as any information relating to an identified or identifiable natural person, where an identifiable natural person is one whose identity can be determined directly or indirectly, especially by reference to an identifier such as a name and surname, his or her personal identification number, location data, an online identifier or on one or a combination of features that are specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Definition of sensitive personal data

Under the DP Law, sensitive personal data is personal data which reveal:

- racial or ethnic origin;
- political opinions, religious or philosophical beliefs;
- membership in a trade union;
- genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data referring to a natural person’s sex life or sexual orientation.

NATIONAL DATA PROTECTION AUTHORITY

The Personal Data Protection Agency (“**DPA**”) was established in 2005 with the Law on Protection of Personal Data dated 2005 (then called the Directorate for Personal Data Protection of the Republic of Macedonia, while with the adoption of the DP Law it became an agency) as North Macedonia’s data protection authority. The DPA is an independent state agency with competence to oversee the implementation of the DP Law, with its registered seat located at:

Boulevard Goce Delcev 18

1000 Skopje, Republic of North Macedonia

Website

azlp.mk

REGISTRATION

The DPA keeps records of all data controllers and data protection officers and publishes them on its website.

Under the Law on Protection of Personal Data dated 2005, data controllers / processors had an obligation to register their databases containing personal data in the Central Registry of Personal Databases (“**Registry**”) maintained by the DPA. With the adoption of the DP Law, this Registry changes in a way that it continues to exist, i.e. continues to be maintained by the DPA, but as a registry of databases involving a high risk (“**High-Risk Records**”), whereas controllers / processors should notify the DPA about their respective high risk databases. It is also envisaged that the provisions of the DP Law governing the High-Risk Records shall cease to apply upon accession of the Republic of North Macedonia to the EU.

The DPA requires entities to report subsequent changes to registration details within 30 days of a change.

The DP Law obliges data controllers / processors and their representatives to maintain records of processing activities with an explicitly prescribed content. However, this obligation is not an obligation generally applicable to all data controllers and data processors. It applies only if data controllers / processors have at least 50 employees or, regardless of their employees’ number, if the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of personal data or personal data relating to criminal convictions and offences.

DATA PROTECTION OFFICERS

Under the DP Law, data controllers and data processors are obliged to appoint a DPO in certain cases, i.e. when:

- processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- core activities of the data controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- core activities of the data controller/processor consist of processing on a large scale of special categories of personal data and personal data relating to criminal convictions and offences.

Data protection officers must:

- inform and advise the data controller or data processor and employees who process data about their duties in accordance with the DP Law;
- monitor compliance with the DP Law, with other national laws and with the policies of the controller/processor;
- increase awareness of data protection practices;
- provide advice on Data Protection Impact Assessment;
- collaborate with the DPA;
- act as a contact for the DPA regarding the adequate collection and processing of personal data and perform other prescribed tasks.

COLLECTION & PROCESSING

The DP Law operates on the basis of the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality and accountability.

The requirement of carrying out the data processing lawfully means that, amongst other, it should be based upon adequate legal ground. Such legal ground is either a data subject's consent (relating to specified, explicit and legitimate purpose/-s) or one of the remaining grounds explicitly prescribed by the DP Law which include:

- necessity of a particular processing for the performance of a contract to which a data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- necessity for compliance with a legal obligation to which the data controller is subject;
- necessity for the protection of the vital interests of the data subject or of another natural person;
- necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, and
- necessity for realization of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

The processing of special categories of personal data is prohibited, unless an exception prescribed with the DP Law applies.

Data subjects are entitled to a range of rights under the DP Law, including right of access, right to rectify, right to erasure (‘right to be forgotten’), right to restriction of processing, right to data portability, right to object, right not to be subject to automated decision making, including profiling.

TRANSFER

Entities may transfer personal data which are subject to processing if the conditions set out in the DP Law are fulfilled and applied.

When transferring personal data to the EU or the European Economic Area (EEA), entities must notify the DPA at least 15 days before the transfer.

Transferring personal data to third countries or international organizations may be conducted only if the DPA deems that the third country or international organization provides adequate levels of protection. When assessing whether the third country or international organization has an adequate level of protection, the DPA considers several parameters, including, among others:

- the rule of law, respect for human rights and fundamental freedoms, relevant legislation and its implementation, professional rules and security measures (including rules for onward transfer), as well as effective and enforceable judgements applied to data subject and effective and administrative and judicial redress for data subjects whose personal data is transferred;
- the existence and effective functioning of one or more independent supervisory authorities in the third country or international organization;
- the international commitments the third country or international organization has entered into, or other obligations arising from legally binding conventions or instruments, in relation to the protection of personal data.

If the above criteria are met by the third country or international organization where the personal data will be transferred, the data transfer can be conducted on the basis of an adequacy decision adopted by the DPA.

The DPA has not yet adopted an adequacy decision. However, the DPA follows the practice of the European Union when it comes to implementing the data protection regulations, and it is expected that any such adequacy decision will be in line with an adequacy decision adopted by the European Commission.

The DP Law itself does not require a special / individual prior approval by the DPA (“**Transfer Approval**”) if an adequacy decision issued by the DPA for the (importing) third country or international organization exists or the below safeguards are provided (on condition that enforceable data subject rights and effective legal remedies for data subjects are available). However, up until this point in time, the DPA has had a conservative approach.

When an adequacy decision has not been adopted, personal data can be transferred to a third country or international organization only if the data controller or data processor apply appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available.

The appropriate safeguards may be provided by:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules in accordance with the DP Law;
- standard data protection clauses determined by the DPA or approved by the European Commission;
- an approved code of conduct or approved certification mechanism pursuant to the DP Law together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards the data subjects’ rights.

Additionally, the DPA could approve the following appropriate safeguards:

- contractual clauses between the data controller and the data processor, as well as the data controller, the data processor or the recipient of the personal data in the third country or international organization; or
- provisions envisaged in administrative agreements between public authorities or bodies which contain applicable and effective data subject rights.

The DP Law also provides a list of derogations for specific situations, based on which a legitimate data transfer out of the Republic of North Macedonia is not conditioned upon a Transfer Approval (e.g. data subject’s consent, enforcement of a contract between a data subject and a data controller, etc.).

Unofficially, starting from 2022, the DPA requires the submission of a performed transfer impact assessment with each request for Transfer Approval when transferring personal data to third countries and international organizations.

Even if the requirements to submit a request for Transfer Approval are not met, but the cross-border transfer of personal data is based on other bases, controllers / processors should still perform a documented transfer impact assessment.

SECURITY

The DP Law requires data controllers and data processors to implement appropriate technical and organizational measures to protect personal data from accidental or illegal destruction, loss, alteration, unauthorized disclosure of personal data or unauthorized access to transferred, stored or otherwise processed personal data. These risks are particularly taken into consideration in order to assess the appropriate level of safety.

The technical and organizational measures include, *inter alia,* as appropriate:

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The data controller and the data processor must always implement the technical and organizational measures relevant to the period in which they are designed and implemented, in accordance with the state-of-the-art technology.

The data controller and the data processor are obliged to apply appropriate levels of technical and organizational measures proportional to the processing activities, while taking into consideration the nature, scope, context and purposes of the processing, as well as the risks with different probability and seriousness for the rights and freedoms of natural persons.

The technical and organizational measures can be classified in two levels:

1. Standard; and

2. High.

The process for managing the system for personal data protection is described in the internally adopted Policy on the System for Personal Data Protection, which should be regularly updated and harmonized in line with any changes in the data controller’s working process.

BREACH NOTIFICATION

Under the DP Law, data controllers are obliged to immediately (and not longer than 72 hours after discovering the data breach) inform the DPA, unless it is likely that the data breach may not pose a risk to the rights and freedoms of natural persons. Data processors are obliged to notify the data controller immediately after discovering the breach.

The notification is submitted on a special form prescribed by the DPA. The information may be gradually submitted without undue delays, only if there was no possibility to submit all of the information at the same time.

If the data breach is deemed to pose a high risk to the rights and freedoms of the natural persons, the data controller must immediately notify the data subject that their personal data has been breached. However, the data controller may not notify the data subject if:

- appropriate technical and organizational measures have been implemented which ensure that the personal data would be unrecognizable to unauthorized persons (e.g. encryption);

- the data controller has implemented additional measures which ensure that there is no longer a high risk to the rights and freedoms of the data subjects; or

- if such notification requires disproportionate effort, in which case a public notification or a similar measure is implemented.

ENFORCEMENT

The DPA has supervisory authority over the protection of personal data, as a systemic and independent control over the legality of the undertaken actions during personal data processing. This supervision entails the inspection, assessment, giving direction and imposing measures to data controllers and processors, through supervisors with the DPA.

The supervision may be:

- regular (announced supervision, conducted in line with the DPA’s annual supervision program);

- extraordinary (unannounced supervision, conducted upon a request, initiative, ex officio or in cases where the supervisors suspect that a breach of the DP Law has occurred); and

- control (conducted within six months after the expiration of the deadline for rectifying violations).

The supervisors enforce DP Law violations by ordering data controllers or processors to remedy violations within a specified time period, or by requesting the initiation of a misdemeanor procedure before the Misdemeanor Commission, taking the seriousness of the offense into consideration. Legal entity fines range from up to 2% and up to 4% of the total annual turnover from the previous financial year, with smaller fines of several hundred euros for the responsible persons at the infringer and the data controllers and processors who are natural persons. Additionally, there is a fine in the range between EUR 1,000 to EUR 10,000 for data controllers which are legal entities who do not adhere to the video surveillance requirements. Entities may dispute DPA fines by initiating proceedings before the Administrative Court of the Republic of North Macedonia.

Individuals are also entitled to bring private claims against controllers and/or processors and request compensation of material or non-material damages suffered due to a breach of the DP Law. Individuals also have the right to lodge a complaint to the DPA and right to an effective judicial remedy against a decision (or lack of) of the DPA concerning them.

The Criminal Code of North Macedonia includes a criminal offense for misuse of personal data punishable by a monetary fine or imprisonment of up to one year, as determined by the court.

ELECTRONIC MARKETING

Under the DP Law, personal data may be processed for electronic (direct) marketing purposes including profiling to the extent connected to the direct marketing only with the data subject’s explicit consent to such processing. The data subject has the right to withdraw his or her consent at any time.

The data subject is entitled to exercise his or her right to object at any time to processing of his or her personal data for such marketing. In situations where the data subject objects to the processing, the personal data shall no longer be processed for such purposes.

ONLINE PRIVACY

The DP Law and the Rulebook on the Security of Personal Data Processing (Official Gazette of the Republic of North Macedonia no. 122/20, **“Security Rulebook”**) apply to online privacy as well.

In line with the Security Rulebook, when using cookies which are not necessary from the service, the data controller should obtain previous consent from the internet user before the cookie is deposited. Data subjects should be informed about the use of cookies and their type, duration, provider, purpose, with which third parties the data is shared, as well as the manner in which cookies can be rejected.

Please note that data controllers and data processors should undertake technical and organizational measures for security of the personal data processing to guarantee the correct identity of the website, as well as the confidentiality of the sent and received information, as prescribed with the Security Rulebook. For example, this would include mandatory use of cryptographic protocol (TLS) for all pages of the website, adoption of a policy for the personal data protection system, etc.

KEY CONTACTS

Ljupka Noveska Andonova
Partner
Karanovic & Partners
T +389 2 3223 870
ljupka.noveska@karanovicpartners.com

Veton Qoku
Partner
Karanovic & Partners
T +389 2 3223 870
veton.qoku@karanovicpartners.com

Ana Kashirska
Senior Associate
Karanovic & Partners
T +389 2 3440 682
ana.kashirska@karanovicpartners.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

NORWAY

Last modified 26 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**") is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

The GDPR was incorporated in the EEA Agreement by a Joint Committee Decision dated July 6, 2018. The new Norwegian Personal Data Act (LOV-2018-06-15-38) ("**PDA**") implements GDPR and became effective as of July 20, 2018.

In addition to implementing GDPR, the PDA includes specific regulations as described below. In connection with the implementation of GDPR, several sector-specific regulations, e.g, in the healthcare sector, has been updated to ensure compliance with GDPR.

The PDA has a similar geographical scope as GDPR article 3 in that it applies to:

1. data controllers and processors established in Norway regardless of whether the processing activities takes place Norway / EEA or not; and

2. processing activities by a data controller or data processor which is not established in the EEA to the extent the processing activity relates to:

a. offering of goods and services to data subjects in Norway, irrespective of whether a payment of the data subject is required; or

b. the monitoring of their behavior, to the extent that such behavior takes place within Norway.

The PDA applies to processing of personal data by controller who is not established in Norway, but in a place governed by Norwegian law according to public international law.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Norwegian Data Protection Authority is:

Datatilsynet

www.datatilsynet.no

Together with other EEA countries (Iceland and Lichtenstein) the Norwegian Data Protection Authority became members of the EDBP however without voting rights and without the right to be elected as chair and vice-chair, for GDPR-related matters.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The government may issue further regulations as regards the duty to appoint a DPO. No such regulations have been issued yet.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;

- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (*ie,* opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Scope

The PDA and GDPR does not apply to processing activities by physical persons for purely private or family purposes or for processing activities within the justice administration sector. For processing activities for journalistic purposes or academic, artistic or literary expressions, only GDPR articles 24, 26, 28, 29, 32 and 40-43 applies, as well as PDA chapter 6 on supervision and complaints and chapter 7 on sanctions and coercive fines.

Age limit to consent to information society services

According to the PDA section 5, the age limit to consent to information society services is 13 years.

Processing of special categories of personal data

Processing of special categories of personal data is allowed when necessary to perform rights or obligations within the field of employment law.

The Norwegian Data Protection Authority may authorize the processing of sensitive personal data where the processing is in the public interest.

The Norwegian Data Protection Authority can also issue specific regulations allowing for the processing of special categories of data.

Processing of information relating to criminal offences

According to the PDA, the processing of information about criminal offences is subject to the regulations as GDPR article 9(2)(a), (c) and (f) as well as the PDA sections 6, 7 and 9, i.e. the same provisions as the processing of special categories of personal data.

Use of personal ID numbers

Personal ID numbers unique identifiers may only be processed where there are reasonable grounds to require proper identification and the use of personal ID numbers is necessary for such identification.

Specific rules on consent

The PDA contains provisions relating to processing of special categories of personal data for e.g., scientific purposes without the consent of the data subject provided that the processing is covered by necessary warranties in accordance with the GDPR Article 89(1). There is no specific general regulation as regards safeguards according to GDPR Article 89, paragraph 1.

Before processing special categories of data, the data controller should consult and seek advice from the Data Protection Officer ("**DPO**") in accordance with GDPR Article 37.

The above-mentioned advice from the DPO must consider whether the processing will meet the requirements of GDPR and other provisions laid down in the Norwegian Implementation Act. The consultation obligation with the DPO does not apply if an assessment has been made of privacy implications according to GDPR Article 35.

The duty to consult with a DPO also applies to the extent that processing of special categories of data for statistics of scientific purposes is based on consent.

Exemption to data subject rights to access and information

The PDA contains some exemption to the right to access and information according to GDPR Article 13-15 to if the information:

a. is of relevance for Norwegian foreign policy or national security;
b. must be kept secret in order to prevent, investigate, disclose and prosecute criminal acts;
c. that is considered that inadvisable that the data subject obtains due to the health situation of the relevant person or the relationship to close relationships of such persons;
d. subject to duty of confidentiality by law;
e. which only is found in text prepared for internal purposes and not disclosed to others;
f. where disclosure would be in breach of obvious and fundamental private or public interests.

Any denial of access according to the above shall be provided by way of a written explanation.

The right of access according to GDPR Article 15 does not apply to the processing of personal data for archival purposes in the public interest, purpose related to scientific or historical research or statistical purposes in accordance with GDPR Article 89. No. 1 so far as:

a. it will require a disproportionate effort to give access; or
b. the right of access will make it impossible or seriously impair the achievement of the specific purposes.

The right to rectification and restriction in accordance with GDPR Article 16 and 18 does not apply to processing for archival purposes in the public domain interest, purposes related to scientific or historical research or statistical purposes in accordance with GDPR Article 89 No. 1 as far as it is likely that the rights make it impossible or seriously impair the achievement of the specific purposes.

The above exemptions do not apply if the processing has legal effects or directly has factual effects for the data subject.

Access to employee email

A separate regulation (FOR-2018-07-02-1108) issued under the Working Environmental Act (LOV-2005-06-17-62) contains the conditions and procedures that have to be followed for accessing employee emails by an employer. Access to employee email can only take place if there is a legitimate interest or if it is necessary to secure daily operations or if

there is a suspicion that the email has been used in such a manner that it is a clear violation of the working relationship or could lead to dismissal or termination of employment.

The employee shall, as far as possible, be given notice and be able to participate when access to email is made.

CCTV surveillance in the workplace

A separate regulation (FOR-2018-07-02-1107) has also been adopted under the Working Environmental Act and contains provisions on the legality of CCTV surveillance in the workplace, notification and deletion obligations, as well as the legality of transfer of CCTV recordings. CCTV monitoring in the workplace may only take place where it is needed to prevent dangerous situations from arising and to safeguard the safety of employees or others, or where there otherwise is a special need for the monitoring. The regulation also applies to dummy cameras.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, Uruguay, New Zealand, Republic of Korea and the United Kingdom.

With the exception of the United Kingdom, these adequacy decisions do not cover data exchanges in the law enforcement sector which are governed by the Law Enforcement Directive (Article 36 of Directive (EU) 2016/680).

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules and standard contractual clauses. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

Please note that pursuant to a recent decision in the Court Justice of the European Union (Case C-311/18 Schrems II) the EU US Privacy Shield Framework may no longer serve as a legal basis for transfers of personal data between the EEA and USA.

On 4 June 2021, the Commission issued modernised standard contractual clauses under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR). These SCCs contain a practical toolbox to comply with the Schrems II judgment; i.e. an overview of the different steps companies have to take to comply with the Schrems II judgment as well as examples of possible ‘supplementary measures', such as encryption, that companies may take if necessary.

These modernised SCCs replace the three sets of SCCs that were adopted under the previous Data Protection Directive 95/46. Since 27 September 2021, it is no longer possible to conclude contracts incorporating these earlier sets of SCCs.

Until 27 December 2022, controllers and processors can continue to rely on those earlier SCCs for contracts that were concluded before 27 September 2021, provided that the processing operations that are the subject matter of the contract remain unchanged.

On 12 December 2022, the European Commission launched the process to adopt an adequacy decision for the EU-US Data Privacy Framework, which will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union in its Schrems II decision.

Once the adequacy decision is adopted, European entities will be able to transfer personal data to participating companies in the United States, without having to put in place additional data protection safeguards.

Hopefully this adoption process will be completed during the spring of 2023.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defense of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and

freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

Data breaches that require notification to the Norwegian DPA, can be notified by completing an online form through Altinn, a Norwegian internet portal for digital dialogue between businesses and public agencies.

The form is available online.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Fines

Fines may be imposed on public authorities. Furthermore the PDA sets out that fines under GDPR will also apply to a breach of GDPR article 10 (processing of data relating to criminal convictions) and 24 (obligation on the controller to implement appropriate technical and organizational measurements to demonstrate that processing is in accordance with GDPR).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*e.g.,* an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to

the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (*eg,* an email address is likely to be ‘personal data’ for the purposes of the Act).

Pursuant to the Marketing Control Act (LOV-2009-01-09-2, Nw: *Markedsføringsloven*) section 15, it is prohibited in the course of trade, without the prior consent of the recipient, to send marketing communications to natural persons using electronic methods of communication which permit individual communication, such as electronic mail, telefax or automated calling systems (calling machines).

Prior consent is however not required for electronic mail marketing where there is an existing customer relationship and the contracting trader has obtained the electronic address of the customer in connection with a sale. The marketing may only relate to the trader’s own goods, services or other products corresponding to those on which the customer relationship is based.

At the time that the electronic address is obtained, and at the time of any subsequent marketing communication, the customer shall be given a simple and free opportunity to opt out of receiving such communications.

‘Electronic mail’ in the context of the Marketing Control Act means any communication in the form of text, speech, sound or image that is sent via an electronic communications network, and that can be stored on the network or in the terminal equipment of the recipient until the recipient retrieves it. This includes text and multimedia messages sent to mobile telephones.

Direct marketing emails must not conceal or disguise the identity of the sender. If the email is unsolicited, it shall clearly state that the email contains a marketing message upon receipt of the message (The Norwegian E-Commerce Act (LOV-2003-05-23-35), Nw: *Ehandelsloven*, section 9).

ONLINE PRIVACY

Traffic Data

Traffic data is defined in Norwegian Regulation relating to Electronic Communications Networks and Electronic Communications Services (FOR-2004-02-16-401, Nw: *Ekomforskriften*) section 7-1 as data which is necessary to transfer communication in an electronic communications network or for billing of such transfer services.

Processing of traffic data held by a Communications Services Provider ('CSP') (Nw: *Tilbyder*) may only be performed by individuals tasked with invoicing, traffic management, customer enquiries, marketing of electronic communications networks or the prevention or detection of fraud.

Traffic Data held by a CSP must be erased or anonymized when it is no longer necessary for the purpose of the transmission of a communication (Electronic Communications Act (LOV-2003-07-04-83) section 2-7 (Nw: *Ekomloven*). However, Traffic Data can be retained if it is being used to provide a value added service and consent has been given for the retention of the Traffic Data.

Location Data

Location data may only be processed subject to explicit consent for the provision of a value added service which is not a public telephony service, and the users must be given understandable information on which data is processed and how the data is used. The user shall have the opportunity to withdraw their consent. See Norwegian Regulation relating to Electronic Communications Networks and Electronic Communications Services section 7-2.

Cookie Compliance

The Electronic Communications Act has been changed in accordance with directive 2009/136/EC regarding the use of cookies. According to section 2-7 b, the user must give their consent before cookies or any other form of data is stored in their browser. The users must receive clear and comprehensive information about the use of cookies and the purpose of the storage or access.

However, obtaining user consent is not required if the cookie solely has the purpose of transferring communication in an electronic network, or if it is deemed to be necessary for the delivery of a service requested by the user. The decision of the Court Justice of the European Union in case C-673/17 (Planet 49) entails that consent to non-essential cookies no longer can be expressed through browser settings, at least if the cookie entails processing of personal data. The National Communications Authority, the authority responsible for supervising the Electronic Communications Act, recommends adhering to the consent regime of GDPR (i.e. freely given, specific, informed and unambiguous) if a website operator is uncertain of its compliance with regards to consent.

The Norwegian Government has proposed changes in relation to obtaining cookie-consent in connection with the proposed new Electronic Communications Act. According to the proposal the definition of a legal consent will be equal to the definition in GDPR (i.e clear opt-in). These changes are expected to enter into force during 2023 and if implemented in accordance with the proposal, the changes will clarify the current uncertainty regarding the consent regime regarding the use of cookies. The Norwegian Government does not preclude that one can provide a general consent for cookies (when required) through browser settings for as long as this is by way of an affirmative action. However, it still remains to be seen whether it is technically and legally possible to implement a general GDPR compliant consent through browser settings.

KEY CONTACTS

Ketil Sellæg Ramberg
Partner
T +47 24 13 15 57
ketil.ramberg@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

PAKISTAN

Last modified 4 January 2024

LAW

Pakistan currently has not enacted data protection legislation per se similar to data protection legislation enacted in other countries of the world, however the Prevention of Electronic Crimes Act, 2016 (“**PECA 2016**”) at present serves the same purpose to a certain extent.

Moreover, a draft of the Personal Data Protection Bill 2023 (“**PDPB**”) has been introduced by the Ministry of Information Technology and Telecommunications with a view to having the same being promulgated into law after public consultation, approval from both Houses of Parliament and receipt of assent from the President of Pakistan.

DEFINITIONS

Definition of personal data

The term “*personal data*” is defined in PECA 2016 in Section 2(xviii) as ““identity information” means an information which may authenticate or identify an individual or an information system and enable access to any data or information system.”

“Data” in PECA 2016 is defined in Section 2(xiii) as ““data” includes content data and traffic data.”

The use of the word ‘include’ in the abovementioned definition of ‘data’ is indicative of the fact that the legislators intended for the definition of ‘data’ to include content data and traffic data in addition to what the typical dictionary meaning and definition of the word ‘data’ is.

Hence, identity information means any piece of information that is capable of authenticating or identifying an individual and enable access to any piece of information that may indirectly assist in authenticating or identifying an individual.

On the other hand, the PDPB defines “*personal data*” as “any information that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that information or other information in the possession of a data controller and / or data processor, including any sensitive or critical personal data. Provided that anonymized, or pseudonymized data which is incapable of identifying an individual is not personal data”.

For the purpose of clarity, “*data subject*” under the PDPB means a natural person who is the subject of the personal data, whereas “*data controller*” means a natural or legal person or the government, who either alone or jointly has the authority to decide on the collection, obtaining, usage, or disclosure of personal data.

In addition, the PDPB defines “*anonymized data*” as personal data which has undergone the irreversible process of transforming or converting personal data to a form in which a data subject cannot be identified. The PDPB defines “*pseudonymisation*” as the processing of personal data in such a manner that the personal data can no longer be attributed

to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

It must be noted, however, that the PDPB is yet to be promulgated into law and therefore the content of the promulgated legislation may differ from the draft.

Definition of sensitive personal data

PECA 2016 does not differentiate between the terms “*personal data*” and “*sensitive personal data*”, and therefore a piece of information that is considered as “*sensitive personal data*” shall be covered under PECA 2016 if the same is capable of being classified as “*identity information*” under the aforementioned legislation.

The PDPB however specifically provides a definition of “sensitive personal data” to mean any personal data relating to: financial information excluding identification number, credit card data, debit card data, account number, or other payment instruments data; health data (physical, behavioural, psychological, and mental health conditions, or medical records); computerized national identity card or passport; biometric data; genetic data; religious beliefs; criminal records; political affiliations; caste or tribe; and an individual’s ethnicity.

It must be noted, however, that the PDPB is yet to be promulgated into law and therefore the content of the promulgated legislation may differ from the draft.

NATIONAL DATA PROTECTION AUTHORITY

There is currently no authority specific to data protection in Pakistan. However, section 16(2) of PECA 2016 authorizes the Federal Investigation Agency (“FIA”) established under the Federal Investigation Agency Act, 1974, along with Pakistan Telecommunication Authority (“**PTA**”) established under the Pakistan Telecommunication (Re-organization) Act, 1996, to enforce PECA and to take action against unauthorized access and use of identity information. PECA 2016 also grants other powers to PTA to regulate the access, use, processing and retention of data through promulgating various rules under PECA 2016.

The PDPB provides for the creation of a National Commission for Personal Data Protection (“Commission”) within six months of the coming into force of the PDPB as law.

REGISTRATION

There is currently no registration requirement.

However, the PDPB, which is yet to be promulgated, confers upon the Commission the power to devise the appropriate registration requirements.

DATA PROTECTION OFFICERS

There is currently no law in force which makes mandatory the appointment of a Data Protection Officer. Alternatively, PECA 2016 provides for the establishment of an investigation agency under section 29, whose “authorized officers” are granted powers of investigation and cognizance, which may be similar to that of a data protection officer in some capacities. The investigation agency under this provision of PECA 2016 is the Federal Investigation Agency (FIA), authorized through rule 3 of the Prevention of Electronic Crimes Investigation Rules, 2018.

However, the PDPB, which is yet to be promulgated into law, recognizes the existence and role of a Data Protection Officer, which shall be determined by the Commission.

COLLECTION & PROCESSING

Section 16(1) of PECA 2016 (“Section 16(1)”), reproduced below for ease of reference, puts restriction on the collection and procession of personal data without the consent of the person whose personal data is being collected and processed:

> “Whoever obtains, sells, possesses, transmits or uses another person’s identity information without authorization shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five million rupees, or with both.”

The PDPB, in addition, provides for the imposition of an obligation upon the data controller to notifythe data subject, in writing, regarding the following: the collection of personal data pertaining to the data subject, along with its description; the legal basis of such data collection and data processing; the retention period; the purpose for such data collection and data processing; information relating to the source of such personal data; information regarding cross border transfer of data; informing the data subject of their rights under the PDPB, including the right to request access to the personal data collected and processed, right to request correction of personal data collected and processed, and provide contact information of the data controller; the choices and means of restricting the processing of personal data;the third parties to whom the personal data may be disclosed; the mandatory or voluntary nature of data collection and data processing; and the consequences of failing to supply mandatory personal data. As per the PDPB, where the processing pertains to critical personal data, the PDPB shall (if implemented in its current form) require the same to be processed in a server or digital infrastructure within Pakistan.

It must be noted, however, that the PDPB is yet to be promulgated into law and therefore the content of the promulgated legislation may differ from the draft.

TRANSFER

Section 16 of PECA 2016 prohibits the transmission of identity information of a person without consent.

Section 4 of PECA 2016 penalizes unauthorized copying and transmission of data with dishonest intentions, with imprisonment up to six months, or a fine up to one hundred thousand rupees, or both.

Section 7 of PECA 2016 penalizes unauthorized copying and transmission of critical infrastructure data with dishonest intentions, with imprisonment up to five years, or a fine up to five million rupees, or both. Under Section 2 of PECA 2016, critical infrastructure data means data that supports or performs a function with respect to a critical infrastructure, namely an asset, facility, system, network or process.

Section 42 of PECA 2016 allows for the Federal Government to transfer data to any foreign government, agency or any international organization for the purposes of investigations or proceedings, and for the collection of evidence concerning offences, upon receipt of a request of the designated investigation agency under PECA 2016.

In addition, Pakistan prohibits data transfers to any country that it does not recognize, including: Israel, Taiwan, Somaliland, Nagorno, Karabakh, Transnistria, Abkhazia, Northern Cyprus, Sahrawi Arab Democratic Republic, South Ossetia and Armenia. This list may change from time to time. Additionally, data transfers to India must be justifiable by the transferor.

Data collated by banks, insurance firms, hospitals, defense establishments and other ‘sensitive’ institutions may not be transferred to any individual or body without authorization from the relevant regulator on a confidential basis. Such data is further regulated by contractual terms. In certain cases, data may not be transferred without authorization from the data subject.

However, banks and financial institutions must maintain confidentiality in banking transactions.

Similarly, the PDPB, which is yet to be promulgated, proposes prohibiting the transfer of personal data to unauthorized persons or systems. Where the transfer of personal data pertains to a transfer to a territory outside of Pakistan, the PDPB would require

the territory where personal data is to be transferred to offer an equivalent degree of personal data protection as that provided for in Pakistan, provided that such data transfer is done in accordance with a framework for the transfer of personal data outside of Pakistan as devised by the Commission.

SECURITY

There are currently no additional data security requirements under the provisions of PECA 2016. However, there are additional requirements under sector specific legislation, such as in the banking and finance sector.

Further, once promulgated, the PDPB would require data collectors and data processors to comply with the standards so prescribed by it for the protection of personal data.

BREACH NOTIFICATION

There is, at present, no requirement to report data breaches to any individual or regulatory body specifically under PECA 2016. However, there are self-reporting requirements under sector specific laws, which may contain the reporting of a breach of personal data.

Additionally, the PDPB would, upon coming into force, require the data controller to notify the Commission regarding any personal data breaches that are likely to result in a risk to the rights and freedoms of the data subject, within 72 hours of knowledge of breach. Moreover, the data processor would similarly be required to intimate any breach of personal data to the Commission, within 72 hours, in the event that the data processor is made aware of such breaches.

ENFORCEMENT

For breaches of provisions of PECA 2016 appropriate relief may be sought through courts of law having jurisdiction in the matter. Specifically, for the breach of personal data and identity information, section 16(2) of PECA 2016 authorizes PTA to secure, destroy, block access to, or prevent transmission of such data if an application is made by the data subject.

Other mechanisms of enforcing data protection also require action by data subjects themselves. An individual may file a complaint with the National Response Centre for Cyber Crime (NR3C) of the Federal Investigation Agency (FIA), which is the law enforcement agency authorized under PECA 2016 and its rules.

Sector specific legislation is enforceable by its respective regulatory or governmental authorities.

Additionally, the PDPB, which is yet to be promulgated, would permit the relevant regulatory authority to exercise all powers required to enable the same to enforce the provisions of the PDPB.

ELECTRONIC MARKETING

The legislation at present does not provide a comprehensive framework to regulate electronic marketing and the processing or transmission of any personal data as a result of electronic marketing. Section 25 of PECA 2016 however prohibits any person from engaging in spamming (including transmission of harmful, fraudulent, misleading, illegal or unsolicited information), though it may be noted that the aforementioned prohibition is only applicable where such spamming is done by a person for a wrongful gain.

Pursuant to the provision of PECA 2016 on spamming, PTA has restricted promotional text messages from telemarketing firms, which now have to provide the recipient with an option to unsubscribe in the promotional message.

ONLINE PRIVACY

PECA 2016 criminalizes unauthorized access to information systems or data, copying or transmission of data and use of identity information. PECA 2016 further criminalizes “*offenses against the dignity of a natural person*,” including the transmission of information through an information system which “*harms the reputation or privacy of a natural person.* ”

Pursuant to the above, PTA has promulgated the Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2021. The purpose of these rules is to allow greater regulation of online content which may be argued to hamper an individual’s privacy and freedom on online platforms. Under section 3 of PECA 2016, the authority under these rules is PTA, which under these rules has very broad powers to examine, block and remove online content under section 3.

Under section 5, PTA also has the power to issue written directions to a social media service provider, to take any such actions for the removal or blocking of online content as it deems fit, and also prescribe timelines to the service provider for compliance with such a direction. If the direction is not complied with within the timeline, PTA may take actions against the service provider including degrading or terminating its services and levying penalties as well. Such a direction by PTA will also take precedence over the community guidelines of an individual service provider.

Additionally, an “e-Safety Bill, 2023” has been drafted by the Ministry of Information Technology and Telecommunication in Pakistan, for the regulation of online content on social network platforms and service providers.

The bill envisages the establishment of an ‘e-Safety Authority’ for enforcing its provisions. This authority shall have various powers to regulate the establishment and registration of and content on social media platforms, to ensure the protection of its users. However, the current discussion draft of the bill contains a broad definition of “ data” and provides for the access of data to the e-safety authority in a broad and arbitrary provision which allows the authority or any person authorised by it to have access to any communication device for the purpose of searching the device and obtaining any information or data, if it has reasonable cause to suspect contravention of the provisions of this bill. In this manner, the proposed bill may allow another authority access to data on online platforms.

KEY CONTACTS

Liaquat Merchant Associates (LMA)
www.lma.com.pk/

Hira Ahmad
Partner
Liaquat Merchant Associates (LMA)
T +92 21 3583 5101-102-103-104
h.ahmad@lma.com.pk

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

PANAMA

Last modified 28 January 2024

LAW

Panama has taken significant legislative steps in regulating data protection. Law No. 81 of March 26, 2019, supplemented by Executive Decree No. 285 of May 28th, 2021 (together the ***Ley sobre Protección de Datos Personales***; the ‘Data Protection Law’), regulates data protection in the Republic of Panama. The Data Protection Law govern the following:

- The principles, rights, obligations, and procedures applicable to the protection of personal data in Panama
- The individuals or legal entities, whether private or public, who are subject to the Data Protection Law, as well as those entities that are classified as “regulated subjects” (*ie*, banks, insurance companies, telecommunication providers, etc.)
- The data subject’s right to access, rectification, cancellation, opposition, and portability
- The fines and penalties applicable to those who violate an individual’s right to data protection

As mandated by the Data Protection Law, it’s expected that several sectoral laws will be modified to include certain data protection terms, such as Rule No. 1-2022, dated February 24th, 2022, which includes special guidelines for the protection of data processed by banks established by the Superintendency of Banks.

In addition to the Data Protection Law, the following general rules govern data protection:

- The Constitution
- The Criminal Code

DEFINITIONS

Definition of personal data

Personal Data is defined by the Data Protection Law as the personal information of an individual that identifies him or makes him identifiable.

Definition of sensitive data

Sensitive Data is defined by the Data Protection Law as the one that refers to the intimate sphere of its owner, or whose improper use could give rise to discrimination or entail a serious risk for the individual, such as information about the racial or ethnic origin, beliefs or religious, philosophical and moral convictions; union membership; political opinions; data related to health, life, sexual preference or orientation, genetic data or biometric data, among others, subject to regulation and aimed at identifying univocally a natural person.

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Regulations are enforced and overseen by:

Panama’s National Authority of Transparency and Access to Information (‘ANTAI’) through the Directorate for the Protection of Personal Data
(Autoridad Nacional de Transparencia y Acceso a la Información)
Del Prado Avenue, Bulding 713, Balboa, Ancon, Panama
T (507) 527-9270 to 74
Protecciondedatos@antai.gob.pa

The National Authority for Government Innovation
(Autoridad Nacional para la Innovación Gubernamental) in matters related to Information and Communications Technology (ICT) supporting ANTAI
61st Street and Ricardo Arango Avenue, Sucre, Arias y Reyes Bulding, Floor 3
Obarrio, Panama
T (507) 520-7400
administracion@innovacion.gob.pa

REGISTRATION

The Data Protection Law does not include any registration or notification requirement prior to the processing of data before Panama’s National Authority of Transparency and Access to Information (“ANTAI”). What it does require, is for data controller’s (known in Panama as the “Responsible of the data treatment”) (*Responsable del tratamiento de datos* in Spanish) to have the data subject’s consent to the processing of said personal data, as a general principle.

DATA PROTECTION OFFICERS

Appointment of a data protection officer is optional under the Data Protection Law for private companies, but required for governmental entities. According to Rule No. 1-2022, banks established in the Republic of Panama are also required to appoint a data protection officer.

COLLECTION & PROCESSING

In Panama, personal information is protected at the constitutional level. The Constitution provides that every person has a right of access to his / her personal information contained in data banks or public or private registries and to request their correction and protection, as well as their deletion in accordance with the provisions of the law. It also states that such information may only be collected for specific purposes, subject to the consent of the person in question, or by order of a competent authority based on the provisions of the law. The disclosure of personal information without consent is also prohibited by the Panamanian Criminal Code. Criminal penalties apply to the disclosure of personal information where the disclosure causes harm to the affected individual.

As per the Data Protection Law, the data subject must consent to the processing of his data and be duly informed of the proposed use of his personal data. Prior to obtaining consent, the data controller must provide the data subject with certain basic information, such as for example: the data controller’s identity and contact information, the proposed use of the data, the data subject's right to revoke consent, recipients of the personal data where the data will be transferred abroad, how long the data will be kept. The consent must be obtained in such a way that allows its traceability with documentation, whether electronic or by any other means that are suitable to the medium of the particular case and can be revoked, without retroactive effect. If the consent of the data subject is given in the context of a sworn statement that also refers to other matters, the consent request will be presented in such a way that it is clearly distinguished from the others, in a comprehensible and easily accessible manner, using a clear and simple language, which will not be binding in any part of the declaration that constitutes an infraction of the Law and its regulation.

The Data Protection Law allows processing of personal data without the data subject's consent, if at least one of the following conditions is met:

- If necessary within an established contrctual relationship

- If needed to fullfil a legal obligation
- If authorized by a sectorial law or regulation
- If necessary to protect the vital interests of the data subject or another individual
- If required by a public entity within the exercise of the functions of the Public Administration in the field of their competences
- If necessary for the satisfaction of legitimate interests pursued by the data controller or by a third party, provided that such interests do not prevail over the interests or fundamental rights and freedoms of the interested party that require the protection of personal data, in particular when the interested party is a minor or a person with a disability
- If the personal data is derived or collected from public domain sources or accessible in public media
- If the personal data is contained in lists related to a category of people that is limited to genera background, such as the participation of a natural person to an organization, their profession or activity, their educational titles, address or date of birth
- If the processing of personal data by private organizations is for the exclusive use of their associates and the entities to which they are affiliated, for statistical purposes, for pricing or others of general benefit to them
- If the processing of information is authorized by law for historical, statistical or scientific purposes

TRANSFER

With regards to personal data, the Constitution states that individuals must give their consent in order for their personal data to be transferred or processed in any way.

The Data Protection Law clearly states that in no case may the data controller or the data processor transfer or communicate the data related to an identified or identifiable person, after seven years have elapsed since the legal obligation of kept said personal data, unless the data subject expressly requests otherwise. Data controllers can only transfer personal data when they have the prior, informed and unequivocal consent of the data subject, with the exceptions included in the Data Protection Law.

Additionally, the Data Protection Law allows for cross-border transfer of personal data, if any of the following conditions are met:

- With the data subject’s consent
- The recipient country or international or supranational organization provides an equivalent or a higher level of protection
- If necessary for the prevention or medical diagnosis, the provision of health care, medical treatment or the management of health services
- If made to any company of the same economic group of the data controller, provided that the personal data is not used for different purposes that originated their collection
- If necessary under an executed or soon to be executed contract in unambiguous interest of the data subject, by the controller and a third party
- If necessary or legally required for the safeguard of a public interest or for the legal representation of the data subject or administration of justice
- If necessary for the recognition, exercise or defense of a right in a judicial process, or in cases of international judicial collaboration
- If necessary for the maintenance or fulfilment of a legal relationship between the data controller and the data subject
- If required to conclude bank or stock transfers, relative to the respective transactions and according to the legislation that is applicable to them
- If the objective is international cooperation among intelligence agencies for the fight against organized crime, terrorism, money laundering, computer crimes, child pornography and drug trafficking
- If the data controller responsible for the data transfer and the recipient adopt mechanisms of binding self-regulation, provided that they are in accordance with the provisions of the Data Protection Law
- If carried out within the framework of contractual clauses that contain mechanisms for protection of personal data in accordance with the provisions set out in the Data Protection Law, provided that the data subject is a party

In all cases, the data controller responsible for the data transfer and the recipient of the personal data will be responsible for the legality of the data processing.

SECURITY

In matters of security, data controllers must establish protocols, safe management and transfer processes and procedures to protect the rights of data subjects under the precepts of this Law. The minimum requirements that must be contained in the privacy policies, protocols and procedures for data processing and transfer that must be met by the data controller, will be issued by the regulator of each sector in accordance with this law.

In the event that the treatment or transfer of personal data is carried out through the Internet or any other electronic, digital or physical means, the data controller or the data processor, whomever applies must comply with the standard certifications, protocols, technical and management measures appropriate to preserve the security in their systems or networks, in order to guarantee the levels of protection of personal data as established by the Data Protection Law.

BREACH NOTIFICATION

If a data controller becomes aware of a security breach, defined as any damage, loss, alteration, destruction, access and in general, any illegal or unauthorized use of personal data, even where such occurs accidentally, that represents a risk for the data’s protection, the data controller must immediately notify such breach to the regulator and affected data subjects, within 72 hours. Data processors also have the responsibility to immediately notify the data controller of any security breach.

The data controller must document any security breach and include at a minimum the following information: i) date of occurrence, ii) the reasons of the breach, iii) the facts related to the situation and its effects, iv) the definitive corrective measures immediately implemented.

The regulator will verify the seriousness of the incident and if required to safeguard the rights of the data subjects, order that the data controller adopt measures, such as the wide dissemination of the incident in the media and/or measures to reverse or mitigate the effects of the incident.

Operators that manage public networks or that provide communication services available to the public shall guarantee in the exercise of their activity the protection of personal data in accordance with the Data Protection Law. They must also adopt the appropriate technical and management measures to preserve the security in the operation of the network or in the provision of their services, in order to guarantee the levels of protection for the personal data that are required by the Data Protection Law, as well as certifications, protocols, standards and other measures established by the respective authorities.

In case there is a particular affectation or violation of the security of the network communication system, the operator that manages such network or provides the communication service will inform the data subjects about said affectation and about the measures to adopt.

ENFORCEMENT

ANTAI, through a Directorate created for this purpose, is empowered to sanction data controllers or data processors that are found to have infringed data subject’s rights, in the course of an investigation of complaints filed and proven against them. Sanctions will be subjected to ANTAI, which will set the amounts of the sanctions applicable to the respective violations, according to the seriousness of them, which they will establish from a thousand US dollars (USD 1,000.00) up to ten thousand US dollars (USD 10,000.00).

ELECTRONIC MARKETING

Law No. 51 of July 22nd, 2008, as amended by Law 82 of November 9, 2012 (“Law 51”), and its bylaws establish in the Executive Decree No. 40 of May 19, 2009 (“Decree 40”) and Executive Decree No. 684 of October 18, 2013 (“Decree 684”) regulate the electronic documents and electronic signatures, as well as the rendering of data storage services, and the certification of the electronic signatures, and adopts other dispositions for the development of e-commerce. It establishes that Companies that sell goods or services in Panama, through the Internet, will be subject to the other provisions of national legislation that apply to them based on the activity they develop, regardless of the use of electronic means for their realization.

With respect to email advertising, Panamanian law requires that all such emails:

- State that they are commercial communications
- Include the name of the sender
- Set forth the mechanism through which the recipient may choose not to receive any further communications from the particular sender

These requirements apply to other promotional offers as well.

Further, although opt-out tools are not prohibited, the client's initial opt-in consent is specifically required if an entity wishes to use the client's email for advertising purposes. Further, although no specific prohibition has been enacted with respect to the use of information for online advertising, obtaining the customer's consent is always preferable.

ONLINE PRIVACY

The existing regulatory framework does not yet address location data, cookies, local storage objects or other similar data-gathering tools.

KEY CONTACTS

Galindo, Arias & Lopez
gala.com.pa/

Ramon Ricardo Arias Porras
Galindo, Arias & Lopez
T +507 303 0303
rrarias@gala.com.pa

Beatriz Cabal
Galindo, Arias & Lopez
T +507 303 0303
becabal@gala.com.pa

Jose Luis Sosa
Galindo, Arias & Lopez
T +507 303 0303
jsosa@gala.com.pa

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

PARAGUAY

Last modified 28 January 2024

LAW

Legal framework

- National Constitution, art. 135, Habeas Data: Any person may file an action to have access to (i) personal data about such person or its property; and (ii) information about the use of such data and purpose for which it is kept, whether it is stored in public or private data registries. Additionally, any person may request the suppression, correction, confidentiality or updating of the data where inaccurate or discriminatory;
- Criminal Code, art. 174 (Unlawful access to computer systems) and art. 175 (Sabotage of computer systems): individuals or entities that unlawfully access or alter personal data contained in databases (computer systems) are criminally liable;
- Law No. 6534/2020 “of protection of personal credit data” (“**Personal Credit Data Protection Law**” or “**Law**”). The previous data protection regulatory regime lead by Law No. 1682/2001 “which regulates the use of private information” as amended by laws No. 1969/2002 and 5543/2015 is no longer in force and was replaced in full by the Personal Credit Data Protection Law (Art. 30 of the Law); and
- Law No. 4868/2013 “Electronic Commerce” **(“Electronic Commerce Law”)** and its regulatory decree No. 1165/2014 **(“Regulatory Decree of the Electronic Commerce Law").**

DEFINITIONS

Definition of personal data

Art. 3 of Personal Credit Data Protection Law defines Personal Data or Personal Information as “information of any type that refers to legal entities or natural persons that are identified or identifiable. An identifiable person shall mean any person who can be identified by means of an identifier or by one or more elements that characterize the physical, physiological, genetics, mental, economic, cultural, or social identity of the data subject. The rights and guarantees of personal data protection shall be extended to legal entities, insofar as they are applicable”.

Definition of sensitive personal data

Sensitive Personal Data is defined as information that refers to the intimate sphere of the data subject, or data that, if misused, may give rise to discrimination or entail a serious risk for the data subject. Personal data is considered sensitive when it reveals aspects such as racial and ethnic origin; religious, philosophical and moral beliefs or convictions; trade union memberships; political opinion; data related to health, life, sexual preference or orientation, genetic or biometric data aimed at uniquely identifying a natural person.

Personal Credit Data Protection Law further defines Credit Data as 'information, positive and negative, related to the credit history of natural persons and legal entities, in relation to credit, commercial and other activities of similar nature, that serves to identify, correctly and unequivocally, the data subject, his/her address, business activity, determine his/her level of indebtedness, compliance with his/her financial obligations and, in general, of his/her credit risks, at any given time'.

NATIONAL DATA PROTECTION AUTHORITY

There is no National Data Protection Authority in Paraguay.

For activities that are considered to be “electronic commerce” as provided by the Electronic Commerce Law, the national authority is the General Direction of Digital Signature and Electronic Commerce – Ministry of Industry and Commerce **(“Electronic Commerce Direction”).**

REGISTRATION

Under the current legislation, no registration is required in order to process or store personal data.

Even though the Electronic Commerce Law does not establish a registration requirement, according to Art. 7 of the Regulatory Decree of the Electronic Commerce Law, the Electronic Commerce Direction has the faculty to gather information from companies that render services via electronic means (such as electronic storage data companies) regarding:

- their commercial activity;
- their identity; and
- other data established in current regulations.

Such companies have the duty to collaborate with the Electronic Commerce Direction and comply with all information requirements (Art. 8, Regulatory Decree of the Electronic Commerce Law).

DATA PROTECTION OFFICERS

Under current legislation, the appointment of Data Protection Officers is not required.

COLLECTION & PROCESSING

Under the current legal regime, it is prohibited to publicize or diffuse sensitive data of people that are explicitly identified or identifiable (Art. 4 of Personal Credit Data Protection Law).

The current regulatory regime allows for private use the collection, storage and processing of personal information when it is lawful, exact, complete, true and updated for the specific purpose for which the data was collected (Art. 7 of the Law). However, the data subject has to give consent to the collection and use of their personal information, to that effect, the data subject has to be informed, clearly and expressly, about the purposes their collected personal data will be processed for. The data subject’s consent may be revoked at any time under the same conditions as it was granted (Art. 6 of the Personal Credit Data Protection Law).

The Personal Credit Data Protection Law specifically regulates personal credit data collection and processing by Credit Data Bureaus. Such bureaus have to be fully authorized and registered by the Central Bank in order to be able render credit reference services (*ie,* provision of data related to personal credit information of persons or entities) and may only provide services to specific users (*eg,* financial entities, banks, credit agencies, etc.) (Arts. 3, 12, 13 and 14 of the Law).

Furthermore, the Personal Credit Data Protection Law establishes that a Credit Data Bureau may process personal data related to financial solvency and credit of persons or entities provided that:

- the data was provided by the data subject; or
- the data subject provided express and written consent; or
- the information is related to information that private or governmental entities have the duty to publish; or
- the information is public (Art. 13 of the Law).

The Personal Credit Data Protection Law also establishes a duty to the person/entity responsible for collecting and/or storing the data, to permanently update (when necessary) any personal information regarding the financial situation, solvency and/or the fulfilment of commercial and financial obligations (Arts. 9 and 11 of the Law). It also provides that the users of Credit Data

Bureaus have the obligation to regularly provide to them, updated data on their credit portfolio clients, especially information related to the compliance with credit obligations, which must be notified within twenty four (24) hours of its cancellation (Art. 14 of the Law).

In addition, the Law establishes that Personal Credit Data which may affect a data subject cannot be stored (and/or publicized) for more than five (5) years from the date of the recorded event (Art. 9 of the Law).

A data subject has the right to:

- access the information and data about themselves, their dependents and/or property;
- know the use and purpose of such data; and
- where data is incorrect, inexact or misleading, request access, prompt correction, rectification, to withdraw consent and object to the processing (Art. 5 of Personal Credit Data Protection Law).

In addition, the Regulatory Decree of the Electronic Commerce Law establishes that the data subject’s express consent is required in order to obtain any personal information (Art. 13). Accordingly, electronic collection, storage and processing data companies (and other companies that render services via electronic means who collect personal data), have the duty to inform to the data subject about:

- the purposes for which the personal data are collected; and
- how the personal data colelcted will be processed.

TRANSFER

The Personal Credit Data Protection Law establishes that international transfers of personal data to a recipient that is in a third country (as defined under the Law), or to an international organization where the guarantees, requirements and/or exceptions established in the Law are not met, is a violation of applicable data protection law and, thus, can be subject to sanctions (Art. 21.x. of the Law).

Under current legislation, there are no other specific provisions that regulate the transfer of private information. However, the transfer of private information is considered as a form of data processing, so the same rules than for collection and processing personal data applies (Art. 3.e. of the Law – definition treatment of data).

SECURITY

Under current legislation, there are no specific security requirements regarding the protection of private information. However, Art. 10 of the Law establishes that the person or entity responsible of the treatment of personal credit data shall guarantee the adoption and implementation of the necessary technical, organization, and security measures to protect the access and integrity of personal data in order to prevent its alteration, loss, commercialization and not authorized access.

The Regulatory Decree of the Electronic Commerce Law also establishes that companies that render services via electronic means (that also collect or process personal or private data), have the duty to:

- inform to the recipient of such data, of the person in charge of its custody and storage; and
- implement secure systems to avoid the unauthorized loss, alteration and/or third party access to such data (Art. 11).

Additionally, such companies have the duty to inform consumers and users (in a transparent, clear and simple manner) regarding the specifics of:

- the level of security and the applicable privacy policy covering the permanent protection of personal data; and
- security measures and technology used to protect the means of payment and the transfer, processing and/or storage of financial data (Art. 12).

BREACH NOTIFICATION

No data breach notification obligation exists under the current data protection regime.

ENFORCEMENT

The current legal regime contemplates the following enforcement mechanisms:

- Without the need of a court order, a data subject has the right to (i) access the information and data about themselves, their dependents and/or property and know how such data is used; and (ii) request the correction and suppression of the information Art. 5 and 8 of Personal Credit Data Protection Law). Data controllers and processors must establish simple, fast, accessible and free of charge procedures, to enable data subjects to exercise their rights. However, where the data subject’s efforts in obtaining the above are unsuccessful, it may bring court actions to compel access to personal data and request the correction, suppression or updating of such data; and
- Violations against obligations established under the Personal Credit Data Protection Law and the Electronic Commerce Law are subject to fines.

The enforcement authorities for the enforcement of the Personal Credit Data Protection Law are the Central Bank of Paraguay ('**BCP**') and the National Secretariat of Consumer and User Defense ('**SEDECO**'). The BCP has authority to further regulate, interpret and enforce the Law (Art. 20 of Personal Credit Data Protection Law).

ELECTRONIC MARKETING

The Electronic Commerce Law requires that all marketing communications and promotional offers:

- state that they are commercial communications;
- include the name of the sender; and
- provide a mechanism through which the recipient may choose not to receive any further communications from the particular sender.

Additionally, the communication shall state that the recipent's private data was obtained without violating privacy rights.

Electronic Marketing is also subject to general marketing and advertising related provisions of the Consumer’s Protection Law.

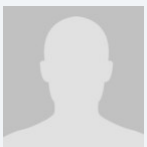
ONLINE PRIVACY

Art. 30.3. of the Electronic Commerce Law requires suppliers of goods and services ,which use data storage and recovery devices, to clearly and thoroughly inform users and consumers about the use of and purposes regarding the collected data and provide data subjects the ability to object to the use(opt-out) of their personal data through a simple procedure and free of charge.

Other than the rule mentioned above, the current legal framework does not specifically address location data, cookies, local storage objects or other similar data-gathering tools.

KEY CONTACTS

Jorge Angulo
Junior Partner
Fiorio, Cardozo & Alvarado Law Firm
jorge.angulo@fca.com.py



Gustavo Arbo
Fiorio, Cardozo & Alvarado Law Firm
gustavo.arbo@fca.com.py

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

PERU

Last modified 26 January 2023

LAW

Article 2 of the Political Constitution of Peru sets forth certain fundamental rights that every person has, including a right to privacy regarding information that affects personal and family privacy, which was the basis for the creation of a law that specifically protects the use of personal data of any natural person and applies to both private and state entities.

The Personal Data Protection Law N° 29733 (PDPL) was enacted in June 2011. In March 2013, the Supreme Decree N° 003-2013-JUS-Regulation of the PDLP (Regulation) was published in order to develop, clarify and expand on the requirements of the PDPL and set forth specific rules, terms and provisions regarding data protection.

Together, the PDLP and its Regulation are the primary data protection laws in Peru.

It should be noted that in 2023, the NDPA published a bill for a new Regulation to the PDPL. The new Regulation is expected to be officially published in 2024 and aims to enhance the protection of personal data under the PDPL by including improvements to contribute to the defense of the protection of personal data considering the rapid development of e-commerce, artificial intelligence, and similar digital technologies.

Further, the law regulating private risk centers and the protection of the owner of the information is Law N° 27489, enacted in 2001 and later amended several times. This law establishes the applicable provisions for activities related to risk centers and companies that handle:

- Information posing higher risks to individuals (*eg*, related to financial, commercial, tax, employment or insurance obligations or background of a natural or legal person that allows evaluating its economic solvency), and
- Sensitive personal data (according to the PDPL)

DEFINITIONS

Definition of personal data

Personal data is defined as information — regardless of whether numerical, alphabetic, graphic, photographic, acoustic — about personal habits or any other kind of information about an individual that identifies or may identify such individual by any reasonable means.

Definition of sensitive personal data

Sensitive personal data includes all of the following:

- Personal data created through biometric data which by itself renders a data subject identifiable
- Personal data regarding an individual's physical or emotional characteristics, facts or circumstances of their emotional or family life, as well as personal habits that correspond to the most intimate sphere

- Data referring to racial and ethnic origin
- Economic income, opinions or political, religious, philosophical or moral convictions
- Union membership
- Information related to physical or mental health, to sexual life or other similar information that affect the data subject’s privacy

NATIONAL DATA PROTECTION AUTHORITY

The Directorate for the Protection of personal data, which is part of the General Directorate of Transparency, Access to Public Information and Protection of Personal Data (NDPA), is the primary agency in charge of enforcing data protection matters.

The NDPA’s current address is:

Scipion Llona 350
Miraflores, L-18
Lima
Peru

Website

REGISTRATION

The National Registry for the Protection of Personal Data (NRPDP) maintains information about personal databases of public or private ownership and publishes a list of such databases to facilitate individuals’ exercise of their rights of access to information, rectification, cancellation, opposition and others regulated in the PDPL and its Regulation.

In addition, the NRPDP maintains records of:

- Communications of cross-border flow of personal data, and
- The sanctions, precautionary or corrective measures imposed by the NDPA

The holders of personal databases must register in the NRPDP providing the following information:

- The name and location of the personal database
- The purposes and the intended uses of the database
- The identification of the owner of the personal database
- The categories and types of personal data to be processed
- Collection procedures and a description of the system for processing personal data
- The technical description of the security measures
- The recipients of personal data transfers

The cross-border transfer of personal data must be notified to the NDPA, including the information required for the transfer of data and registration of the database.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer in the private sector (only in the public sector). However, when a company registers its personal database with the NDPA, it can report that it has a Security Manager of that database.

COLLECTION & PROCESSING

The collection and processing of personal data requires the data subject’s prior, informed, express and unequivocal consent. The consent may be expressed through electronic means.

The collection and processing of sensitive personal data requires the data subject’s prior, informed, express and unequivocal consent, and must be expressed in writing.

The data subject’s consent is not necessary if any of the following are true:

- The data are compiled or transferred for the fulfillment of governmental agency duties
- The data are contained or destined to be contained in a publicly available source
- The data are related to credit standing and financial solvency, as governed by applicable law (Law N° 27489)
- A law is enacted to promote competition in regulated markets, under the powers afforded by the Framework Law for Regulatory Bodies of Private Investmenton Public Services (Law N° 27332), provided that the information supplied does not breach the user’s privacy
- The data are necessary for a contractual, scientific or professional relationship with the data subject, provided that such data is necessary for the development and compliance with such relationship
- The data are needed to protect the health of the data subject, and data processing is necessary, in circumstances of risk, for prevention, diagnosis, and medical or surgical treatment, provided that the processing is carried out in health facilities or by professionals in health sciences observing professional secrecy
- The data are needed for public interest reasons declared by law or public health reasons (both must be declared as such by the Ministry of Health) or to conduct epidemiological studies or the like, as long as dissociation procedures are applied
- The data are dissociated or anonymized
- The data are used by a nonprofit organization with a political, religious, ortrade union purpose, and refer to the data of its members within the scope of the organization´s activities
- The data are necessary to safeguard the legitimate interest of the data subject orthe data handler
- The data are being processed for purposes linked to money laundering and terrorist financing or others that respond to a legal mandate
- In the case of economic groups made up of companies that are considered subjects obliged to inform, the data is processed in accordance with the rules that regulate the Financial Intelligence Unit, so that they may share information with each other about their respective clients to prevent money laundering and financing of terrorism (as well as in other instances of regulatory compliance, establishing adequate safeguards on the confidentiality and use of the information exchanged)
- When the treatment is carried out in a constitutionally valid exercise of the fundamental right to freedom of information
- Others expressly established by law

If the data controller outsources the processing of the personal data to a third party (*ie,* a processor), such party must also comply with the relevant requirements of the PDLP (*eg*, to maintain personal data as confidential and to use the personal data only for the purposes authorized and modify inaccurate information).

Upon termination or expiration of the outsourcing agreement, the personal data processed must be deleted, unless the data subject provides express consent to do otherwise.

The processing of personal data by cloud services, applications and infrastructure is permitted, provided compliance with the provisions of the PDPL and its Regulation is guaranteed.

TRANSFER

Where personal data is transferred to another entity, recipients must be required to handle such personal data in accordance with the provisions of the PDPL and its Regulation.

Generally, data subject consent is required.

Cross-border transfers

The transferring entity may not transfer personal data to a country that does not afford adequate protection levels (protections that are equivalent to those afforded by the PDPL or similar international standards). If the receiving country does not meet these standards, the sender must ensure that the receiver in the foreign country is contractually obligated to provide 'adequate protection levels’ to the personal data, such as via a written agreement that requires that the personal data will be protected in accordance with the requirements of the PDPL, or under one of the following circumstances:

- In accordance with international treaties in which Peru is a party
- For purposes of international judicial cooperation or international cooperation among intelligence agencies to combat
    - Terrorism
    - Drug trafficking
    - Money laundry
    - Corruption
    - Human trafficking, and
    - Other forms of organized crime
- When necessary for a contractual relationship with the data subject, or for a scientific or professional relationship
- Bank or stock transfers concerning transactions in accordance with the applicable law
- The transfer is performed to protect, prevent, diagnose or medically or surgically treat the data subject, or to perform studies of epidemiology or the like, provided a data dissociation procedure has been applied
- The owner of the personal data has given its prior, informed, express and unequivocal consent to the transfer to the inadequate jurisdiction
- Other exempt purposes established by the Regulations

For both domestic and cross-border transfers, the recipient must assume the same obligations as the transferor of the personal data. The transfer must be formalized, such as by binding written contract, and capable of demonstrating that the holder of the database or the data controller communicated to the recipients the conditions in which the data subject consented to their processing.

As an alternative to the above mentioned “adequate transfer” requirement, a Data Controller may execute with a Data Processor (or other Data Controller) the standard contractual clauses already approved by the Peruvian Data Protection Authority, which include several obligations and declarations regarding the data transfer between the parties.

SECURITY

Database holders and data handlers must adopt technical, organizational and legal measures necessary to guarantee the security of the personal data they hold. The measures taken must ensure a level of security appropriate to the nature and purpose of the personal data involved.

The Agency has passed a Directorial Resolution N° 019-2013-JUS/DGPDP (hereafter, the 'Security Directive'). This Security Directive establishes different standards depending on the features of the database, including:

- Number of data subjects whose data are contained in the database
- Number of fields of the database (eg, name, address, phone number)
- Existence of sensitive data
- Owner of the database (an individual or entity)

The following security measures must be taken with respect to the loss of a personal data bank:

- Backup copies of personal data must be made to allow recovery in case of loss or destruction
- Any recovery of personal data, from the backup, must have the authorization of the person in charge of the personal data bank
- Proof of recovery of personal data must be performed to verify that backup copies can be used if they are required

For digital information, it is important to mention that the computer systems that handle databases or process personal data must include in their operation records that keep all types of interaction with logical data, so as to identify the users, changes, consultations, starting and closing hours of a session and other actions that are carried out. These records will allow the access of competent, authorized and identified personnel only.

Further, it is necessary to establish the following:

- Security measures related to the authorized accesses to the data by procedures of identification and authentication that guarantee the confidentiality and integrity of the data

- Necessary mechanisms for correct application of the procedures for making backup copies and recovery of the data in order to guarantee the reconstruction in the status they had at the time of the loss or destruction

The applicable measures in which the information must be processed, stored or transmitted—taking into account the controls, policies, standards and recommendations related to physical and environmental security—are established in the following documents:

- Peruvian Technical Standards 'NTP- ISO/IEC 17799: 2007 EDI. Technology of Information. Code of Good Practice for the management of the security of the information. 2nd Edition'
- 'NTP ISO/IEC 27001: 2008 EDI Technology of Information. Security Techniques. Systems of Management of Information Security. Requisites.'

BREACH NOTIFICATION

The holder of a database (and processor, where applicable) is required to implement security measures to prevent the unauthorized access to personal data.

As a consequence, an implied obligation would be to adopt all corrective measures in the event of a data breach to minimize the damages it may cause to the data subjects. For that reasons, the Security Directive establishes security measures against:

- The loss of the personal database, and
- An unauthorized processing of the personal database

In this way, any case of data breach should be communicated to the data subjects as soon as it is confirmed. The database owner must inform the data subject of 'any incident that significantly affects their property or their moral rights', as soon as the occurrence of the incident is confirmed.

The minimum information to be provided in a notice includes a description of:

- The incident
- Personal data disclosed
- Recommendations to the data subject
- Corrective measures implemented

Further, it should be noted that the NDPA does not provide any terms or guidelines for submitting a mandatory or voluntary report in case of a digital security incident, nor does it contemplate any sanctions for lack of reporting.

Mandatory breach notification

Pursuant to Emergency Decree 007-2020, which approves the Digital Trust Framework, with the intent to strengthen cybersecurity ("Emergency Decree"), public administration entities, digital service providers in the financial sector, utilities (electricity, water and gas), healthcare and passenger transportation, internet service providers, and other providers of critical activities (economic and/or social activity whose interruption has serious consequences on the health and safety of citizens, on the effective functioning of essential services that maintain the economy, society and government, or affects the economic and social prosperity in general) as well as educational services must comply with the following: (a) notifying the National Centre for Digital Security (the “National Centre”) about every digital security incident; and, (b) reporting and collaborating with the NDPA in case of a digital security incident that involves personal data.

A Digital Security Incident is defined under the Emergency Decree as an “event or series of events that may compromise the trust, economic prosperity, protection of individuals and their personal data, the information, among other assets of the organization, through digital technologies”.

However, the following should be noted:

- According to the first and second final complimentary provisions of the Emergency Decree, regulations and guidelines will be issued in order to provide more information on the provisions and obligations contained in the Emergency Decree. To date no regulations have been issued.
- As previously mentioned, there are no terms or guidelines regarding the notification procedure before the National Centre, except for a brief statement on the Secretary’s website, stating that the reporting entity -when notifying a data breach- must include its identification information and all relevant information regarding the data breach that may help evaluate the incident, including supporting documents.

Considering the above, while formal content requirements for reporting breaches to the National Centre and the NDPA (as detailed above) exist, currently, due to the lack of regulations and issued guidelines, practically these are not being demanded by the relevant authorities.

ENFORCEMENT

The General Directorate of Sanctions (part of the NDPA) instructs on and resolves, in the first instance, violations and imposes sanctions as well as conducts and develops the research phase according to Article 115 of the Regulation of the PDLP.

The General Directorate for the Protection of personal data (also part of the NDPA) resolves in the second and last instance the sanctioning procedure and its decision exhausts the administrative route.

Possible sanctions for breaching data protection standards vary depending on the nature or magnitude of the offense:

- The fine applicable to minor infringement ranges from S/ 2,575 to S/ 25,750 (approximately between USD 700 and USD 7,000).
- The fine applicable to severe infringements ranges from S/ 25,750,000 to S/ 257,500 (approximately between USD 7,000 and USD 70,000).
- The fine applicable to very severe infringements ranges from S/ 257,500 to S/ 515,000 (approximately between USD 70,000 and USD 140,000).

Please note that the NDPA imposes fines considering the value of the Tax Unit for the year in which the offense is committed. The value for the Tax Unit for the current year 2024 is S/ 5,150 (approximately USD 1,400).

The NDPA is also authorized to impose additional fines up to S/ 51,150 (approximately USD 14,000), if the offender, despite being found liable and sanctioned as a consequence thereof, fails to remedy the unlawful practice. These are applicable in addition to civil and criminal liability.

ELECTRONIC MARKETING

The PDPL does not expressly regulate electronic marketing. However, the PDPL does apply to electronic marketing activities if personal data is processed as a result.

If consent is obtained through electronic media, the notice requirements can be met by publishing accessible and identifiable privacy policies with the relevant consent language and mechanism. The PDPL establishes the possibility of obtaining express consent by presenting the option to agree with the privacy policies in clickable ways (*eg*, by clicking, ticking a box).

Written consent may be provided by other options, including:

- Through an electronic signature
- A written document possible to read or print
- A mechanism or procedure that allows one to identify the subject and to receive his consent through a written text
- A pre-established text as long as it is easily visible, legible and written in simple language

The laws governing electronic signatures are:

- Law N° 27291
- The Digital Certificates and Signatures Law (Law N° 27269)

- Supreme Decree N° 052-2008-PCM

Note that expressing the will in any of the regulated forms does not eliminate the other requirements of consent referring to that consent must be informed, and freely given.

According to the article 58.1 of Consumer Protection Code Law N° 29571, the following commercial activities require prior, informed, express and unequivocal consent to promote products and services:

- Use of call centers
- Use of telephone call systems
- Bulk text messages or
- emails Telemarketing services

As to date, it is permitted to obtain personal information from public sources or by licit means in order to contact the data subjects to get their consent for the aforementioned commercial activities. Notwithstanding the foregoing, whenever the data subject does not grant its consent for commercial activities, it must not be contacted again for those purposes. Furthermore, easily accessible and free mechanisms must be implemented to allow the data subjects to revoke their consent for the commercial purposes.

However, a bill has been proposed, which would modify the aforementioned article 58.1, so that advertising could only be sent to consumers who request to receive such and grant the sender unequivocal, free, informed and express consent to be contacted for marketing purposes. So, a data subject’s information (i.e. telephone numbers and e-mails) could be used for marketing purposes only if the data subject has consented to be contacted by the sender for marketing purposes.

ONLINE PRIVACY

The PDPL does not expressly regulate online privacy, including cookies and location data. However, the PDPL will apply if personal data is collected and processed using these mechanisms.

This requires that the use and deployment of cookies, location data or another personal data that will be collected must comply with data privacy laws. The data subject’s consent must be obtained before cookies and/or location data can be used.

With respect to criminal law enforcement, Legislative Decree N° 1182 permits the National Police of Peru to access the location and geolocation of mobile phones or electronic devices of similar nature in cases of *flagrante delicto*.

It establishes the obligation for public communications services providers and public entities to keep the data from their users derived from telecommunication services during the first 12 months in computer systems an additional period of 24 months in an electronic storage system. Such service providers are bound to provide the location and geolocation data immediately, 24 hours a day, 365 days of the year, under warning of being liable to the responsibilities regarded by law in the event of noncompliance.

KEY CONTACTS

Ricardo Escobar
Partner
DLA Piper Pizarro Botto Escobar
T +1 511 616 1200
rescobar@dlapiperpbe.com

Daniel Flores
Associate
DLA Piper Pizarro Botto Escobar
T +1 511 616 1200
dflores@dlapiperpbe.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

PHILIPPINES

Last modified 2 January 2024

LAW

The Data Privacy Act of 2012 (“**Act**” or “**DPA**”) or Republic Act No. 10173, which took effect on 8 September 2012, is the governing law on data privacy matters in the Philippines.

In 2022, two bills (House Bill No. 892 and House Bill No. 898) were filed in the House of Representatives of the Philippines, seeking to amend the DPA. The proposed amendments under House Bill No. 892 broadly include:

- Increasing the penalties (both the period of imprisonment and monetary fines) for violations of the DPA; and
- Providing for perpetual absolute disqualification as a penalty for a public official or employee who violates provisions of the DPA.

On the other hand, the proposed amendments under House Bill No. 898 broadly include:

- Defining biometric and genetic data.
- Expanding the exclusions on the applicability of the DPA.
- Redefining “sensitive personal information” to include biometric and genetic data, and labor affiliation. Clarifying the extraterritorial application of the DPA by specifying clear instances when the processing of personal data of Philippine citizens and / or residents is concerned.
- Defining the digital age of consent to process personal information as more than fifteen (15) years, applicable where information society services are provided and offered directly to a child.
- Including the performance of a contract as a new criterion of the lawful basis for processing of sensitive personal information.
- Allowing Personal Information Controllers (“**PIC**”) outside of the Philippines to authorize Personal Information Processors (“**PIP**”) or any other third party in the country, in writing, to report data breaches to the National Privacy Commission (“**NPC**”) on behalf of the PIC.
- Modifying criminal penalties under the DPA, giving the proper courts the option to impose either imprisonment or fine upon its sound judgment.

The said bill remains pending before the Philippine House of Representatives.

A further bill was filed in 2022 and is pending before the Philippine Senate (Senate No. 1367) likewise seeking to amend the DPA. Specifically, the bill seeks to exclude the applicability of the DPA to personal information and sensitive personal information that are necessary to address a health crisis during a period of a declared national emergency or pandemic.

In 2021, the Philippine House of Representatives approved a bill (House Bill No. 9651) proposing amendments to the DPA similar to that of House Bill No. 898. The said bill has been transmitted to the Philippine Senate for concurrence the same year but remain pending as of date.

Given the rigorous process of passing a law in the Philippines there are no indications that any of these pending bills will be passed into law within the next 12 months.

DEFINITIONS

Definition of personal information

Personal Information is defined in the Act as ‘any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.’

The Act, in addition to defining ‘Personal Information’ that is covered by the law, also expressly excludes certain information from its coverage. These are:

- information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:
    - the fact that the individual is or was an officer or employee of the government institution;
    - the title, business address and office telephone number of the individual;
    - the classification, salary range and responsibilities of the position held by the individual; and
    - the name of the individual on a document prepared by the individual in the course of employment with the government.
- information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;
- information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;
- Personal Information processed for journalistic, artistic, literary or research purposes (intended for a public benefit);
- information necessary in order to carry out the functions of a public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act ("**CISA**");
- information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or *Bangko Sentral ng Pilipinas* to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; and
- Personal Information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.

Definition of sensitive personal information

"Sensitive Personal Information" is defined in the Act as Personal Information:

- about an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- about an individual’s health, education, genetic or sexual life of a person, or to any proceeding for any offence committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns, and specifically established by an executive order or an act of Congress to be kept classified.

NATIONAL DATA PROTECTION AUTHORITY

The National Privacy Commission (“**NPC**” or **Commission**) is an independent body mandated to administer and implement the Act, and to monitor and ensure compliance of the country with international standards set for personal data protection. The NPC was created in 2016 and the implementing rules and regulations of the Act took effect in the same year.

REGISTRATION

Data Protection Officer and Data Processing Systems

NPC Circular No. 2022-04 (effective January 2023) provides for mandatory registration of the Data Protection Officer (“ **DPO**”) and the data processing systems (“**DPS**”) for PICs or PIPs that:

- employ two hundred and fifty (250) or more persons;
- process Sensitive Personal Information of one thousand (1,000) or more individuals; or
- process data that will likely pose a risk to the rights and freedoms of data subjects.

Registration is done via the NPC’s online platform i.e. the NPC Registration System or NPCRS accessible here.

Entities that are not subject to mandatory registration may opt to voluntarily register their DPO and DPS.

A PIC or PIP who is not subject to mandatory registration and does not undertake voluntary registration shall submit a sworn declaration. The Commission, through an order, may require a PIC or PIP to submit supporting documents related to this submission.

A covered PIC or PIP shall register its newly implemented DPS or inaugural DPO in the NPCRS within twenty (20) days from the commencement of such system or the effective date of such appointment.

In the event that a covered PIC or PIP seeks to make minor amendments to its existing registration information, which include updates to an existing DPS, or a change in DPO, the PIC or PIP shall update the NPCRS within ten (10) days from the system update or effective date of the appointment of the new DPO.

A Certificate of Registration issued upon completion of the registration process shall be valid for one (1) year from its date of issue.

PICs and PIPs are mandated to prominently display their NPC registration at the main entrance of their place of business and on their websites, if the PIC and PIP have an online presence.

DATA PROTECTION OFFICERS

The PIC of an organization must appoint a person or persons who shall be accountable for the organization’s compliance with the Act, and the identity of such person or persons must be disclosed to the data subjects upon the latter’s request. The implementing rules and regulations of the Act likewise require any natural or juridical person or other body involved in the processing of personal data to designate an individual or individuals who shall function as DPO, compliance officer or otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security. The Act does not specifically provide for the citizenship and residency of the DPO. The Act likewise does not specifically provide for penalties relating to the incorrect appointment of DPOs.

The NPC has published guidelines on the designation of the DPO.

COLLECTION & PROCESSING

The collection and processing of Personal Information must comply with the general principle that Personal Information must be:

- collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;

- processed fairly and lawfully;
- accurate, relevant and, where necessary for purposes for which it is to be used the processing of Personal Information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;
- adequate and not excessive in relation to the purposes for which they are collected and processed;
- retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed:
    - provided that Personal Information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods, and
    - provided, further, that adequate safeguards are guaranteed by said laws authorizing their processing.

In addition, the processing of Personal Information must meet the following criteria, otherwise, such processing becomes prohibited:

- the data subject has given his or her consent;
- the processing of Personal Information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the PIC is subject;
- the processing is necessary to protect vitally important interests of the data subject, including life and health;
- the processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
- the processing is necessary for the purposes of the legitimate interests pursued by the PIC or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

The processing of Sensitive Personal Information is prohibited, except in the following cases:

- the data subject has given his or her specific consent prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
- the processing is provided for by existing laws and regulations, provided that such regulatory enactments guarantee the protection of the Sensitive Personal Information and the privileged information, and the consent of the data subjects is not required by law or regulation permitting the processing of the Sensitive Personal Information or the privileged information;
- the processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

- the processing is necessary to achieve the lawful and non-commercial objectives of public organizations and their associations, provided:
    - such processing is only confined and related to the bona fide members of these organizations or their associations;
    - the Sensitive Personal Data are not transferred to third parties; and
    - the consent of the data subject was obtained prior to processing.
- the processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of Personal Information is ensured; or
- the processing concerns such Personal Information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

TRANSFER

Each PIC is responsible for Personal Information under its control or custody that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

Transfers may involve either data sharing or outsourcing arrangements. “Data sharing” is the disclosure or transfer to a third party of Personal Information under the custody of a PIC or PIP. In the case of the latter, such disclosure or transfer must have been upon the instructions of the PIC concerned. The term excludes “outsourcing,” or the disclosure or transfer of personal data by a PIC to a PIP.

Data sharing and outsourcing arrangements must be undertaken in accordance with the requirements under the Act, which includes the execution of the appropriate agreements. The NPC has likewise issued a circular which provides guidelines on data sharing agreements, including the contents thereof.

SECURITY

The PIC must implement reasonable and appropriate organizational, physical and technical measures to protect Personal Information against any type of accidental or unlawful destruction, such as from accidental loss, unlawful access, fraudulent misuse, unlawful destruction, alteration, contamination and disclosure, as well as against any other unlawful processing.

The determination of the appropriate level of security must take into account the nature of the Personal Information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation.

In addition, the security measures to be implemented must include the following, which are subject to guidelines that the NPC may issue:

- safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;
- a security policy with respect to the processing of Personal Information;
- a process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and
- regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

The PIC is obligated to ensure that third parties processing Personal Information on its behalf shall implement the security measures required by the Act.

The obligation to maintain strict confidentiality of Personal Information that are not intended for public disclosure extends to the employees, agents or representatives of a PIC who are involved in the processing of such Personal Information.

BREACH NOTIFICATION

The PIC is required to notify both the regulator (which is the NPC) and the affected data subjects within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the PIC or PIP that, a personal data breach requiring notification has occurred.

A security incident is treated as a reportable data breach if Sensitive Personal Information or other information has been acquired by an unauthorized person, and:

- such Personal Information may, under the circumstances, be used to enable identity fraud; and
- the PIC or the NPC believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

The notification shall at least describe the nature of the breach, the Sensitive Personal Information possibly involved, and the measures taken by the entity to address the breach. The notification shall also include measures taken to reduce the harm or negative consequences of the breach, the representatives of the PIC, including their contact details, from whom the data subject can obtain additional information about the breach, and any assistance to be provided to the affected data subjects.

Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. The NPC may also authorize postponement of notification where such notification may hinder the progress of a criminal investigation related to a serious breach.

There can be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of Sensitive Personal Information will harm or adversely affect the data subject. In either case, the Commission must be notified within the 72-hour period based on available information.

The full report of the personal data breach must be submitted within five (5) days from notification, unless the PIC is granted additional time by the Commission to comply.

Notification is not required if the NPC determines:

- that notification is unwarranted after taking into account compliance by the PIC with the Act and the existence of good faith in the acquisition of Personal Information; or
- in the reasonable judgment of the NPC, such notification would not be in the public interest or in the interests of the affected data subjects.

In April 2022, the NPC launched the Data Breach Notification Management System (DBNMS), an interface that facilitates tracking and submission of personal data breach notifications and annual security incident reports.

ENFORCEMENT

The NPC is responsible for ensuring compliance of the PIC with the Act. It has the power to receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any Personal Information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report. Additionally, the NPC can issue cease and desist orders, impose a temporary or permanent ban on the processing of Personal Information, upon finding that the processing will be detrimental to national security and public interest.

The NPC, however, cannot prosecute violators for breach of the Act for which criminal penalties can be imposed. The Department of Justice is tasked with the prosecution for violations of the Act that are punishable with criminal sanctions.

The following actions are punishable by the Act with imprisonment in varying duration plus a monetary penalty:

- processing of Personal Information or Sensitive Personal Information:
  - without the consent of the data subject or without being authorized by the Act or any existing law; or
  - for purposes not authorized by the data subject or otherwise authorized under the Act or under existing laws;
- providing access to Personal Information or Sensitive Personal Information due to negligence and without being authorized under this Act or any existing law;
- knowingly or negligently disposing, discarding or abandoning the Personal Information or Sensitive Personal Information of an individual in an area accessible to the public or has otherwise placed the Personal Information of an individual in its container for trash collection;
- knowingly and unlawfully, or violating data confidentiality and security data systems, breaking in any way into any system where Personal and Sensitive Personal Information is stored;
- concealing the fact of such security breach, whether intentionally or by omission, after having knowledge of a security breach and of the obligation to notify the NPC pursuant to Section 20(f) of the Act;
- disclosing by any PIC or PIP or any of its officials, employees or agents, to a third party Personal Information or Sensitive Personal Information without the consent of the data subject and without malice or bad faith; and
- disclosing, with malice or in bad faith, by any PIC or PIP or any of its officials, employees or agents of unwarranted or false information relative to any Personal Information or Sensitive Personal Information obtained by him or her.

In August 2022, the NPC issued a Circular on Administrative Fines for data privacy infractions committed by PICs and PIPs.

ELECTRONIC MARKETING

In 2008, the Department of Trade and Industry, the Department of Health, and the Department of Agriculture issued a joint administrative order implementing the Consumer Act of the Philippines (Republic Act No. 7394) and the E-Commerce Act (Republic Act No. 8792). The Joint DTI-DOH-DA Administrative Order No. 01 (the ‘Administrative Order’) provides rules and regulations protecting consumers during online transactions, particularly on the purchase of products and services. It covers both local and foreign-based retailers and sellers engaged in e-commerce.

The Administrative Order particularly requires retailers, sellers, distributors, suppliers or manufacturers engaged in electronic commerce with consumers to refrain from engaging in any false, deceptive and misleading advertisement prohibited under the provisions of the Consumer Act of the Philippines.

In line with the Administrative Order’s provision on fair marketing and advertising practices, retailers, sellers, distributors, suppliers or manufacturers engaged in electronic commerce are mandated to provide:

- fair, accurate, clear and easily accessible information describing the products or services offered for sale such as the nature, quality and quantity thereof;

- fair, accurate, clear and easily accessible information sufficient to enable consumers to make an informed decision whether or not to enter into the transaction; and

- such information that allows consumers to maintain an adequate record of the information about the products and services offered for sale.

A data subject must be provided with specific information regarding the processing of his personal data for direct marketing. In fact, the data subject shall have the right to object to the processing of his or her personal data, including processing for direct marketing.

In 2022, the NPC, together with other government agencies, issued Joint Administrative Order No. 2022-01 or the Guidelines for Online Businesses Reiterating the Laws and Regulations Applicable to Online Businesses and Consumers (the “ **Guidelines**”). The Guidelines define the responsibilities of online sellers, merchants, or e-retailers under the Act, and seeks to ensure privacy protection and transparency, legitimate purpose and proportionality in data collection and processing.

ONLINE PRIVACY

The Cybercrime Prevention Act of 2012 (“CPA”) is the first law in the Philippines which specifically criminalizes computer crimes. The law aims to address legal issues concerning online interactions. The CPA does not define, nor does it particularly refer to online privacy, however, it penalizes acts that violate an individual’s rights to online privacy, particularly those interferences against the confidentiality, integrity and availability of computer data and systems.

Section 4(c)(3) of the CPA, which provides that unsolicited commercial communications is generally a cybercrime offense punishable under the CPA, was struck down by the Supreme Court for violating the constitutionally guaranteed freedom of expression.

All data to be collected or seized or disclosed will require a court warrant. The court warrant shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce showing that there are:

- reasonable grounds to believe that any of the crimes penalized by the CPA has been committed, or is being committed, or is about to be committed;
- reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and
- no other means readily available for obtaining such evidence.

The integrity of traffic data shall be preserved for a minimum period of six months from the date of the transaction.

Courts may issue a warrant for the disclosure of traffic data if such disclosure is necessary and relevant for the purposes of investigation in relation to a valid complaint officially docketed.

No law in this jurisdiction currently deals with the subject of location data.

Philippine law, including the Act, presently do not define the term “cookies” nor regulate their use. The NPC, however, has opined that cookies, when combined with other pieces of information, may allow an individual to be distinguished from others and may, therefore, be considered as Personal Information. To the extent that cookies are considered as Personal information, the Act may be applicable and consent of the data subjects must be secured prior to (or as soon as practicable and reasonable) the collection and processing of Personal Information, subject to certain exceptions.

KEY CONTACTS

Romulo Mabanta Buenaventura Sayoc & De Los Angeles
www.romulo.com/

Catherine Beatrice O. King Kay
Partner
Romulo Mabanta Buenaventura Sayoc & De Los Angeles
T +63 2 8555 9555
Catherine.Kingkay@romulo.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

POLAND

Last modified 17 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

The Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by the GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretations and enforcement practices among Member States.

Territorial Scope

Primarily, the application of the GDPR depends on whether an organisation is established in the EU. An 'establishment' may take a wide variety of forms and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organisation that it is not established in the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the EU where the processing activities are related "to the offering of goods or services" (Article 3(2)(a)) (no payment is required) to those data subjects or "the monitoring of their behaviour" (Article 3(2)(b)) to the extent their behaviour takes place in the EU.

As a member of the European Union, Poland implemented the EU Data Protection Directive 95/46/EC in the Personal Data Protection Act of 29 August 1997 (consolidated text: Journal of Laws of 2016, item 922, hereinafter: “ **previous PDPA**”).

In relation to GDPR, on 12 September 2017, two bills on personal data protection were published in Poland. The first one was passed into law on 25 May 2018 as the new Personal Data Protection Act of 10 May 2018 (Journal of Laws of 2019, item 1781 (“**PDPA**”), while the second one was passed into law on 4 May 2019 as the Act on amendments to sectorial acts accompanying the GDPR of 21 February 2019, containing amendments to over 160 sectorial regulations, including banking, insurance and labour law (Journal of Laws of 2019, item 730, hereinafter: the “**Implementing Act**”).

The two new pieces of legislation are aimed at implementing the GDPR into the Polish legal order, as well as regulating matters in which the GDPR leaves a certain amount of freedom for EU Member States. The new PDPA establishes a new supervisory body – the President of the Office for Personal Data Protection (hereinafter: the “**Polish DPA** ”), which has a much wider range of powers than the previous DPA (the Inspector General for the Protection of Personal Data – hereinafter: the “**Inspector General**”).

A number of provisions of the Telecommunications Act of 16 July 2004 (consolidated text: Journal of Laws 2018, item 1954, hereinafter: the “**Telecommunications Act**”) are applicable to the processing of personal data by providers of publicly available telecommunications services and a number of sector-specific statutes relating to, among other things, employment and banking matters also contain specific regulations on the processing of personal data.

The amendments to the sectorial regulations included in the Implementing Act affected, among others, employment, banking and insurance regulations. The Implementing Act was passed on 21 February 2019 and entered into force on 4 May 2019.

Several provisions of the law on clinical trials of medicinal products for human use of 9 March 2023 (Journal of Laws 2023, item 605) are also applicable to the processing of personal data. When carrying out clinical trials that are scientific research, it is allowed to limit the application of the provisions of articles 15, 16, 18 and 21 of the GDPR. Those restrictions may be imposed if it is likely that the rights set out in the aforementioned provisions will prevent or seriously hinder the achievement of the objectives of the clinical trial which is a scientific study, and if those restrictions are necessary to achieve those objectives.

According to the amendment of the Polish Labour Code (consolidated text: Journal of Laws 2023, item 1465), the employer may introduce sobriety tests on employees if necessary to ensure the protection of life and health of employees or other persons or the protection of property. The employer processes information about the date and exact time of the sobriety test and its result only if this is necessary to ensure the protection of property, and stores this information in the employee's personal file for a period not exceeding one year from the date of its collection.

DEFINITIONS

Personal data is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The Implementing act does not include any local derogations to the definitions set out in GDPR.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the CNIL in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29

Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The President of the Office for Personal Data Protection.

Office of the President for Personal Data Protection
Urzad Ochrony Danych Osobowych
Stawki 2
00-193 Warsaw
Poland

Tel. +48 22 531 03 00
Fax +48 22 531 03 01
kancelaria@uodo.gov.pl

Helpline (in Polish only): phone no. +48 606-950-000 is open from Monday to Friday from 10 am to 2 pm.

The Office of the President is open from Monday to Friday from 8 am to 4 pm.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg,* processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Under the previous PDPA (in force until May 25, 2018), as a general rule, data controllers that process personal data were obligated to notify the Inspector General about the data filing system containing that data. The Inspector General kept a register of data controllers and data filing systems, which was available to the public.

This obligation does not longer exists under the new PDPA and the Implementing act.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale
- Its core activities consist of processing sensitive personal data on a large scale

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have expert knowledge (Article 37(5)) of data protection laws and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

According to the new PDPA, the appointment of a Data Protection Officer (DPO) must be notified to the supervisory authority within 14 days. The notification should include the name and email address of the DPO or his or her phone number. Any changes to the information provided or the dismissal of a DPO should also be notified within 14 days. The entity who appointed the DPO shall make available the DPO's details on its website or in a generally accessible manner at a place of pursuit of activity (if it does not have its own website). According to official guidance from the Polish DPA, the contact details of the DPO should be easily accessible, not hidden somewhere in long documents such as a privacy policy etc.

The Implementing act includes the possibility to designate a person to replace the DPO during their absence (*eg* , temporary absence). However, it would be necessary to inform the Polish DPA about the designation in the same way as about the designation of a DPO. All rules and requirements for DPOs, such as the ones stated in article 37 of the GDPR or the obligation to inform the Polish DPA are also applicable to this person.

If a person was officially appointed as an Information Security Officer (ABI) under the previous PDPA, this person automatically became a DPO for the data controller until September 1, 2018, and provided that the appointment was notified to the President of the Office before that date, the person continues to serve as a DPO after that date.

If the data controller is obliged to appoint a DPO in accordance with Article 37 of the GDPR but did not appoint one under the previous PDPA, the appointment of the DPO should have taken place and been notified to the President of the Office before July 31, 2018.

COLLECTION & PROCESSING

Data protection principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal basis under article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous,*" and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special category data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent

- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal convictions and offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a secondary purpose

Increasingly, organizations wish to re-purpose personal data – *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (privacy notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)

- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the data subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg*, commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision taking, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. Necessary for entering into or performing a contract
b. Authorized by EU or Member State law
c. The data subject has given their explicit (*ie,* opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The new PDPA includes some derogations from the GDPR. However, the draft of the Implementation act is likely to introduce more provisions which elaborate on the provisions of the GDPR on the collection and processing of personal data. It is important to note that the Polish legislator has decided to include derogations regarding labour law both in the new PDPA and in the Implementation act.

The new PDPA contains provisions amending, among others, the Labour Code. These provisions provide for circumstances under which the employer can carry out video surveillance, email monitoring and other employee monitoring activities. Video surveillance may be implemented if it is necessary to ensure the safety of employees or the protection of property or production control or to keep information, the disclosure of which could cause damage to the employer, confidential. Monitoring of work emails may be implemented if it is necessary to ensure maximum work efficiency and the proper use of work tools made available to the employees. The scope, means and purposes of the employee monitoring must be provided to the employees via workplace regulations or other, exhaustively listed, means at least two weeks before the monitoring starts. The legality of a particular monitoring scheme should be assessed on a case-by-case basis.

The new PDPA also prescribes the maximum retention period of the information obtained from video monitoring (it must not be stored indefinitely). The mater can be retained for three months after the recording took place, unless the recording constitutes (or may constitute) evidence in legal proceedings. In this case, the material may be stored until the final decision in the proceedings is issued. In relation to the retention period of information obtained via any other form of employee monitoring, the general rules of the GDPR apply - the material can be retained as long as is reasonably needed for the purposes for which it was collected. The remaining changes to the Labour Code are included in the Implementation act.

For example, the employer may process the personal data of its employees or job applicants referred to in Article 9(1) with consent however only if the data was given on the data subject's own initiative. Another significant amendment is to the scope of data requested when applying for a job. Although address as well as parents' names are no longer needed, contact details should be provided. Changes in video surveillance would allow an employer to locate cameras in sanitary areas upon prior consent from the enterprise trade union or the employee representative who has been chosen in the way prescribed by an employer. However, the monitoring shall not cover the premises made available to the enterprise trade union.

TRANSFER

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1) of GDPR). Currently, adequacy decisions have been issued with regard to the following countries or territories: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay, New Zealand and Japan.

The European Commission recently released its draft adequacy decision on the EU-US Data Privacy Framework (“EU-US DPF”), which, once formally adopted, would recognise that the United States ensures an adequate level of protection for personal data transferred from the EU to organisations certified under the EU-US DPF.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident,
d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

The Implementing Act does not include any derogations from the GDPR.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to the affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include, where possible, the categories and approximate numbers of individuals and records concerned, the name of the organisation’s data protection officer or other contact, the likely consequences of the breach, and the measures taken to mitigate any harm (Article 33(3)).

Controllers are also required to keep records of all data breaches (Article 33(5)) (irrespective of whether they are notified to the supervisory authority) and permit audits of the records by the supervisory authority.

In Poland, the breach notification obligations under the Telecommunications Act were replaced by the breach notification obligations under the terms specified in Commission Regulation (EU) No. 611/2013 of 24 June 2013 regarding measures applicable to the notification of personal data breaches under Directive 2002/58/ EC of the European Parliament and of the Council on privacy and electronic communications (Regulation 611/2013).

A personal data breach should be reported by the provider of telecommunications services to the Polish DPA immediately, and no later than 24 hours after the detection of the personal data breach. This deadline results from Article 2 section (2) of Regulation 611/2013. Because this period is shorter than the period indicated in the GDPR, telecommunications undertakings will have to make every effort to send the information required by law within 24, not 72, hours. Therefore, the personal data breach should be notified electronically by filling out the appropriate form.

If a data breach could have a negative impact on the rights of a subscriber or end user (i.e. a natural person), the service provider should also - immediately (i.e. without undue delay) - inform the subscriber or end user about the breach (in addition to informing the Polish DPA) in accordance with Regulation 611/2013.

Under the new Electronic Communications bill, the breach notification obligations continue to be superseded by the breach notification obligations under Commission Regulation (EU) No. 611/2013, so relevant provisions remain unchanged.

ENFORCEMENT

In 2021, the Polish DPA issued seventeen administrative fines. Most of them were connected with a failure of an entity to provide information to or cooperate with the Polish DPA , as well as not having sufficient technical and organisational measures to ensure information security.

The biggest fine of 2021 was imposed on a company that provides comprehensive, integrated media and telecommunications services. Its infringement consisted in the failure to implement appropriate technical and organisational measures to ensure the security of personal data processed in cooperation with a courier service provider. The large number of data breaches involved the loss of correspondence with personal data or the delivery of correspondence to the wrong recipient. The company’s data controller reported the breaches to the supervisory authority and notified the affected individuals two or even three months after they occurred. The company was fined EUR 245,000.

Another fine was issued on 14 October 2021. The Polish DPA had become aware of a data protection breach following a complaint against a bank. It turned out that correspondence sent by the bank through a courier service containing personal data (e.g. first name, surname, PESEL number, home address, account numbers and identification numbers of customers) had been lost. The bank had failed to report the incident to the Polish DPA and provide adequate notice to the data subjects and was fined EUR 78,000.

Another decision was issued against an insurance company for failing to report a personal data breach to the Polish DPA and failing to notify the data subject of the breach. The breach was caused by an employee of a financial intermediary sending an insurance needs analysis and an insurance offer, including data such as first name, surname, PESEL number, city, postal code and information on the subject of the insurance, by e-mail to the wrong recipient. The fine was EUR 35,300.

Another fine resulting from a failure to report a personal data breach to the Polish DPA was imposed on a generator, distributor and retailer of electricity. The breach involved sending an email with an unencrypted, non-password-protected attachment containing the personal data of several hundred people. The sender of the email was an associate of the company, which was fined EUR 30,000.

The last of the major fines imposed in 2021 concerned the National School of Judiciary and Public Prosecution, whose data controller failed to implement sufficient technical and organisational measures related to its training platform website. During a test migration to a new platform, the data of more than 50,000 individuals had been exposed on the Internet. The Polish DPA imposed a fine of EUR 22,200.

In 2022, the Polish DPA issued ten decisions imposing administrative fines which, similarly to the previous year, concerned the failure to provide information to the Polish DPA, lack of cooperation with the Polish DPA, and the use of insufficient technical and organisational measures to ensure information security.

So far, the highest fine of 2022, i.e. EUR 1,000,000, was imposed on an electricity and gas trading company, which sells electricity and gas to both business and household end users. The company failed to implement appropriate technical and organisational measures, but also did not properly verify its data processor. The Polish DPA found that unauthorised persons had managed to access and siphon off customer data and blamed both the controller and the processor for the personal data breach affecting more than 100,000 individuals for five days. As a result, the processor was also fined EUR 53,000.

Another fine was imposed on a bank which did not report a personal data breach to the Polish DPA in a timely manner, despite the fact that around 10,500 people were affected. In its decision, the Polish DPA emphasised that it was not necessary for the risk to have actually materialised, but the mere fact that it could have, was sufficient. The bank was fined EUR 118,000.

One recent decision concerned a telecoms operator that failed to report a data breach to the Polish DPA within 24 hours in accordance with the provisions of Telecommunications Act. The company’s data controller also did not notify the affected individuals. The breach occurred during the process of concluding a contract, as an email containing a copy of the contract and its annexes was sent to an address incorrectly indicated by the customer. This was not the first time the entity had not notified the Polish DPA of a data breach by the required deadline, which also had an impact on the fine, which was EUR 53,000.

The same telecoms operator is also the owner of a company providing prepaid and postpaid wireless voice, text and data communications services throughout Poland. This case started in 2019 when the Polish DPA imposed a fine of EUR 444,000 for the lack of appropriate technical and organisational measures to ensure the security of the data it was processing. The company lodged an appeal following the decision and as a result the administrative court stated that the Polish DPA should re-assess the amount of the fine. Now the company has to pay EUR 374,000.

ELECTRONIC MARKETING

Electronic marketing activities are subject to the regulation of Polish data protection law, i.e. the Act of 18 July 2002 on Providing Services by Electronic Means (consolidated text: Journal of Laws of 2018, item 123, hereinafter: “PSEM”) and the Telecommunications Act.

The processing of personal data for its own marketing purposes by a data controller (as well as other companies from the group) may be based on Article 6 sec. 1(f) of the GDPR, i.e. the legitimate interests of the data controller, and it does not require separate consent. However, the data subject may always object to such processing. Nevertheless, if marketing activities relate to products and services of third parties, prior consent for such processing is necessary.

Apart from consent to the processing of personal data (if it is required), the PSEM imposes an obligation to obtain separate consent to the sending of commercial information by electronic means, (e.g. by email and SMS) to a specified recipient (natural person). Therefore, a service provider is obliged to obtain the relevant consent before sending the commercial information (by email or SMS) to a natural person. On the other hand, it is permitted to send such information without prior consent to recipients that are legal persons to a general email address (such as office@company.com) and to a specific employee's business email address (such as name.surname@company.com). According to the Implementing Act, the consent under the PSEM must comply with the GDPR requirements as regards the format. Sending commercial information without consent is considered to be an act of unfair competition and a service provider should be able to provide evidence that it has obtained consent.

Pursuant to the Telecommunications Act, using end telecommunications devices (for instance, to present a marketing offer during a telephone call) or automated calling systems for direct marketing requires the obtaining of another consent declaration from the recipient (subscriber or end user). In practice, the relationship between the abovementioned regulations (especially between the provisions of the new PDPA and the Telecommunications Act) and the scope of particular consent declarations that should be obtained by service providers is not perfectly clear in this regard. However, it seems that, generally, the consent to direct marketing by means of telecommunications devices and automated calling systems should be obtained separately from the consent to the processing of personal data (if required) and to consent to the sending of commercial information by electronic means. According to the Implementing Act, the consent of the subscriber or the end user must comply with the GDPR requirements as regards the format.

According to Introductory Provisions of Electronic Communications bill, the issue of direct marketing will be regulated in a single act, namely in Article 393 of the Electronic Communications Act. At the moment, this issue is covered by two acts: Article 172 of the Telecommunications Act and Article 10 of the PSEM. This gives rise to interpretative doubts as to whether an entity is obliged to obtain two separate consents for marketing communications, or whether the obligation to obtain different consents for communications depends on the means of communication.

The existing Article 172 of the Telecommunications Acts and Article 393 of the bill transpose both Article 13(1) and Article 13(3) of the ePrivacy Directive into the Polish legal order. The provision of Article 13(3) of the Directive gives Member States the right to choose (particularly in the context of telemarketing) whether to apply an opt-in (required consent to communicate) or opt-out (required objection to cease communication) system to other forms of communication than electronic communication in their legal order. Different countries in the European Union have adopted different systems in this area. Hence, it seems reasonable to regulate this issue in a single provision of Article 393 of the Electronic Communications Act instead of regulating it in Article 172 of the Telecommunications Acts and repealing Article 10 of the PSEM.

Under the proposed provision, it is prohibited to use:

1. automatic calling systems; or
2. telecommunication terminal equipment, in particular in the use of interpersonal communication services,

for the purpose of sending unsolicited commercial information, including direct marketing, to a subscriber or end-user unless prior consent has been given.

ONLINE PRIVACY

Regulations under Electronic Communications bill concerning online privacy remain unchanged. The Telecommunications Act regulates the collection of transmission and location data and the use of cookies (and similar technologies).

Transmission data

The processing of transmission data (understood as data processed for the purpose of transferring messages within telecommunications networks or charging payments for telecommunications services, including location data, which should be

understood as any data processed in a telecommunications network or as a part of telecommunications services indicating the geographic location of the terminal equipment of a user of publicly available telecommunications services) for marketing telecommunications services or for providing value-added services is permitted if the user (i.e. subscriber or end user) gives his or her consent.

Location data

In order to use data about location (understood as location data beyond the data necessary for message transmission or billing), a provider of publicly available telecommunications services has to:

- Obtain the consent of the user to process data about location concerning this user, which may be withdrawn for a given period or in relation to a given call, or
- Anonymize this data.

A provider of publicly available telecommunications services is obliged to inform the user, prior to receiving its consent, about the type of data about location which is to be processed, about the purpose and time limits of the processing, and whether this data is to be passed on to another entity in order to provide a value-added service.

Processing data about location may only be performed by entities that:

- Are authorized by a public telecommunications network operator
- Are authorized by a provider of publicly available telecommunications services
- Provide a value-added service

Data about location may be processed only for purposes necessary to provide value-added services.

Cookies

The use and storage of cookies and similar technologies is only allowed on the condition that:

- The subscriber or the end user is directly informed in advance in an unambiguous, simple and understandable manner about:
- The purpose of storing and the manner of gaining access to this information
- The possibility to define the condition of the storing or the gaining of access to this information by using settings of the software installed on his or her telecommunications terminal equipment or service configuration
- The subscriber or end user, having obtained the information referred to above, gives his/her consent, and
- The stored information or the gaining of access to this information does not cause changes in the configuration of the subscriber's or end user's telecommunications terminal equipment or in the software installed on this equipment (the end user may grant consent by using the settings of the software installed in the final telecommunications device that he/she uses or by the service configuration)

The consent of the subscriber or end user is not required if storage or gaining access to cookies is necessary for:

- Transmitting a message using a public telecommunications network
- Delivering a service rendered electronically, as required by the subscriber or the end user

Entities providing telecommunications services or services by electronic means may install software on the subscriber’s or end user’s terminal equipment intended for using these services or use this software, provided that the subscriber or end user:

- Is directly informed, before the installation of the software, in an unambiguous, simple and understandable manner, about the purpose of installing this software and about the manner in which the service provider uses this software
- Is directly informed, in an unambiguous, simple and understandable manner, about the manner in which the software may be removed from the end user’s or subscriber’s terminal equipment
- Gives its consent to the installation and use of the software prior to its installation

According the current draft of the second act, the consent of the subscriber or the end user must comply with the GDPR requirements as regards the format. The legislative procedure is still ongoing and we will update you once the final version of the amendments takes shape.

Enforcement and sanctions

A company that processes transmission data contrary to the Telecommunications Act or fails to meet obligations to obtain consent to process data about location or to store and to gain access to cookies may be subject to a fine of up to 3% of the company’s revenues for the previous calendar year. The fine is imposed by the President of the OEC. In addition, the President of the OEC may impose a fine on a person holding a managerial position in the company (such as a member of the management board) of up to 300% of his or her monthly remuneration.

Enforcement and sanctions

Failing to meet the obligations to obtain consent to direct marketing by means of telecommunications devices and automated calling systems may be subject to a fine of up to 3% of the revenues of the fined company for the previous calendar year. The fine is imposed by the President of the Office of Electronic Communication (hereinafter referred to as the President of the OEC). In addition, the President of the OEC may impose a fine on a person holding a managerial position in the company (such as a member of the management board) of up to 300% of his or her monthly remuneration.

Sending marketing information by electronic means without the consent of the recipient may be subject to a fine of up to PLN 5,000 (approx. EUR 1,200) under the provisions of the PSEM and is considered to be an act of unfair competition (*ie* , a practice that infringes collective consumer interests) and thus may be subject to a fine of up to 10% of the revenues of the fined company for the previous calendar year (subject to separate regulations).

KEY CONTACTS

Ewa Kurowska-Tober
Partner, Global Co-Chair Data Protection, Privacy and Security Group
T +48 22 540 74 1502
ewa.kurowska-tober@dlapiper.com

Magdalena Koniarska
Senior Associate
T +48 22 540 78 19
magdalena.koniarska@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

PORTUGAL

Last modified 17 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A Regulation (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

Currently, processing of personal data in Portugal is governed by GDPR and Law no 58/2019 of 8 August, ensuring the execution of GDPR in Portugal. However, local supervisory authority (CNPD) issued the Decision 494/2019 deciding not to apply certain provisions of such law as they were considered in contradiction with GDPR:

- article 2(1) and (2): scope of the Law;
- article 20(1): duty of secrecy;
- article 23: processing of personal data by public entities for different purposes;
- article 28(3)(a): consent of employee in an employment context;
- article 37(1)(a)(h)(k) and (2): misdemeanors and applicable sanctions;
- article 38(1)(b) and (2): misdemeanors and applicable sanctions;
- article 39(1) and (3): misdemeanors and applicable sanctions;
- article 61(2): connection between the expiry of consent and termination of the agreement (for existing agreements);
- article 62(2): revocation of provisions requiring prior authorization or notification to CNPD with effect from the date of entry into force of the GDPR.

Furthermore, Law no 59/2019 of 8 August contains provisions related with personal data processing for purposes of prevention, detection, investigation and repression of criminal offenses and for purposes of execution of criminal sanctions, transposing EU Directive 2016/680 of the European Parliament and the Council of 27, April, 2016.

Relevant data protection provisions in the context of electronic communications may also be found in Law 41/2004, of 18 August (Law on the processing of personal data and the protection of privacy in the electronic communications, as amended by Law 46/2012, of 29 August and enacted pursuant to Directive 2002/58/EC) (with subsequent amendments arising from Article 2 of Directive 2009/136/EC).

DEFINITIONS

Personal data is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **lead supervisory authority**. Where there is cross-border processing of personal data (*ie,* processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called lead supervisory authority (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Comissão Nacional de Proteção de Dados (‘National Commission for the Protection of Data’. also known as ‘CNPD’).

Av. D. Carlos I, 134 - 1.°

1200-651 Lisboa

T +351 21 392 84 00

F +351 21 397 68 32

geral@cnpd.pt

www.cnpd.pt

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

Under the prior Personal Data Protection Law data controllers who processed personal data should notify such activity to the supervisory authority (CNPD), unless a specific exemption applies. However, such obligations are, as general rule, no longer applicable.

Under Law no 58/2019 of 8 August, the implementation of video surveillance systems with sound recording is not allowed except in cases where the monitored premises are closed or there is prior authorization from the supervisory authority.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale
- Its core activities consist of processing sensitive personal data on a large scale

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have expert knowledge (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

In accordance with Law no 58/2019 of 8 August, the appointment of a Data Protection Officer (DPO) shall follow the requirements provided in article 37 (5) of GDPR. No professional certification is required and the DPO is bound by professional secrecy. In addition to the functions described in GDPR, DPO’s shall ensure the conduction of audits, inform the users of the importance of data breaches detection and ensure the relation with the data subjects in relation to matters covered by GDPR and data protection national laws.

For the purposes of the mandatory notification of the data protection officer to the supervisory authority, in the context of Article 37 (7) of the GDPR, the supervisory authority established the applicable procedure for notification. A specific form made available by the supervisory authority on its website should be completed and submitted online (the form is available here).

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency principle)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation principle)
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (data minimization principle)
- Accurate and where necessary kept up-to-date (accuracy principle)
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (storage limitation principle)
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (integrity and confidentiality principle)

The controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous,*" and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organizations wish to re-purpose personal data – *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymization

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, while others only apply in quite limited circumstances. Controllers must provide information on action taken in response to

requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg,* commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision taking, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

1. Necessary for entering into or performing a contract
2. Authorized by EU or Member State law
3. The data subject has given their explicit (*ie,* opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Personal data may only be processed if any of the GDPR lawful bases apply.

Moreover, the data controller must provide the data subject with all the relevant processing information under the GDPR.

In accordance with Law no 58/2019 of 8 August, the processing of children’s personal data based on consent in the scope of the direct provision of information of society services is only allowed where children are 13 years of age or above. Below 13 years, legal representatives’ consent is required.

Regarding the processing of health and genetic data, such data may only be processed on a need to know basis. In the cases provided for by Article 9(2)(h) and (i) GDPR (ie, where the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care of treatment or the management of health or social care systems or for reasons of public interest in the area of public health), the processing must be carried out by or under the responsibility of a professional who is subject to the obligation of secrecy or by other person bound by a confidentiality obligation, and appropriate information security measures must be ensured. The access to health and genetic data is exclusively made through electronic means unless in case of technical impossibility or under express instructions contrary from the data subject, not being allowed the subsequent transfer or disclosure.

Without prejudice of specific laws and regulations stating the mandatory implementation of video surveillance systems, under Law no 58/2019 of 8 August, the same shall only be implemented for purposes of people and goods protection and for compliance with the legal requirements provided in Law no. 34/2013 of 16, may as well as in Law no 58/2019 of 8 August.

The Personal data retention period is provided by law or regulation or, in case there is no specific law or regulation, it will correspond to the period in which the personal data is needed in view of the purposes of processing. In case the personal data is needed for purposes of evidence of contractual obligations or of other nature, personal data shall only be retained until the limitation period of the respective rights has not elapsed.

Specific legal provisions apply in the scope of employment relationships, notably in relation to video surveillance systems and processing of biometric data.

As concerns data subjects' rights, these shall follow GDPR requirements, establishing Law no 58/2019 of 8 August that the right to data portability provided for in Article 20 of the GDPR only comprises the personal data provided by the respective data subjects and shall be provided, wherever possible, in an open format.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay, New Zealand, Japan and the United Kingdom (with a “sunset clause”).

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes among others binding corporate rules and standard contractual clauses. The EU-US Privacy Shield Framework does not constitute an appropriate safeguard for transferring personal data to the USA since the European Commission Decision 2016/1250 (which was the legal basis for the EU-US Privacy Shield) has been invalidated by the European

Court of Justice on 16 July 2020 (Case C-311/18, *Schrems II*). The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. Explicit informed consent has been obtained
b. The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
d. The transfer is necessary for important reasons of public interest
e. The transfer is necessary for the establishment, exercise or defense of legal claims
f. The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
g. The transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject. Notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State. A transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

Transfers to non-EU/EEA countries or international organizations follow GDPR rules. In respect of transfers of personal data to third countries or international organizations, where the processing is necessary for compliance with a legal obligation and where it is carried out by public entities in the exercise of authority powers, said transfers shall be considered as in the public interest.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The security measures shall follow GDPR provisions. Law no 58/2019 of 8 August also provides that health databases or centralised registers based on single platforms should meet the security and integrity requirements provided for by the GDPR.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification to the supervisory authority is not executed within 72 hours, it shall be accompanied by the reasons for the delay.When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

Personal data breach notifications are required in the circumstances provided in Article 33 GDPR. The Portuguese supervisory authority (CNPD) set out the procedure for a personal data breach notification. A specific form on the supervisory authority's website should be completed and submitted to notify data breaches (the form is available here). The supervisory authority makes also available a form which allows a previously submitted notification to be amended (the form is available here).

Also Law 41/2004, of 18 August (as amended) establishes that companies that provide electronic communications services accessible to the public shall, without undue delay, notify the Data Protection Authority (CNPD) of a personal data breach. When the personal data breach may affect negatively the subscriber’s or user’s personal data, companies providing electronic communications services to the public should also, without undue delay, notify the breach to the subscriber or user so that they can take the necessary precautions.

For these purposes, a negative effect on personal data exists when the breach may result namely in theft or identity fraud, physical harm, significant humiliation or damage to reputation.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- The basic principles for processing including conditions for consent
- Data subjects’ rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data
- Certain orders of a supervisory authority

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

CNPD is the supervisory authority responsible for the enforcement of personal data protection laws and regulations in Portugal. Failure to comply with applicable data protection and privacy legal requirements may result in criminal, civil and administrative liability. Law no 58/2019 of 8 August contains provisions related with civil administrative and criminal liability :

(a) The use of personal data in a manner that is incompatible with the purposes of collection, unauthorized access, or deviation of personal data; the vitiation or erasure of personal data; the insertion of false data, the violation of the duty of secrecy and disobedience, constitute crimes punishable by a prison sentence of up to four years or a fine of up to 480 days. In general terms, legal persons and similar entities have criminal liability.

(b) Any person who has suffered damages due to the unlawful processing of personal data or any other act that violates the provisions of the GDPR or of the national law on personal data protection, has the right to compensation from the data controller or the processor for the damage suffered.

(c) Very serious administrative offences shall be punishable with a fine:

- From EUR 5,000 to EUR 20,000,000 or 4% of the total worldwide annual turnover, whichever is higher, in the cases of large companies
- From EUR 2,000 to EUR 2,000,000 or 4% of the total worldwide annual turnover, whichever is higher, in the case of SMEs
- From EUR 1,000 to EUR 500,000, in the case of natural persons

Serious administrative offences shall be punishable with a fine:

- From EUR 2,500 to EUR 10,000,000 or 2% of the total worldwide annual turnover, whichever is higher, in the cases of large companies
- From EUR 1,000 to EUR 1,000,000 or 2% of the total worldwide annual turnover, whichever is higher, in the cases of SMEs
- From EUR 500 to EUR 250,000, in the case of natural persons

However, that local supervisory authority issued the Decision 494/2019 deciding not to apply certain provisions of Law no 58/2019 of 8 aAugust, notably the ones related with the sanctions applicable to the administrative offenses as were considered in contradiction with GDPR. As so, local supervisory authority, will apply the sanctions described in GDPR.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. In February 2021, the Council of the European Union agreed on a draft Regulation, opening the trilogue phase. It is uncertain how long this phase will last and the ePrivacy Regulation is not expected to enter into force before 2023, therefore it

will not be applicable until at least 2025. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

As established under Law 41/2004, of 18 August (as amended), sending unrequested communications for direct marketing purposes to natural persons is subject to express prior consent of the subscriber or user (that is, the opt-in rule applies). This includes use of automated calling and communications that do not rely on human intervention automatic call devices, fax or electronic mail, including SMS, EMS, MMS and other similar applications.

As regards direct marketing communications to legal persons, these are allowed insofar as opt-out is offered. Legal persons may refuse future communications and request registration in the non-subscribers list.

This does not prevent the supplier that has obtained its clients’ data and contacts in connection with the sale of a product or service to use such data for direct marketing of its own products or services or products or services similar to the ones provided.

Nevertheless, the supplier shall ensure that these clients are given the opportunity to object to the use of such data, free of charge, clearly and explicitly, and in an easy manner, at the time of the respective collection, and on each message (when the client did not opt-out initially upon collection of the data).

Moreover, sending electronic mail for direct marketing purposes via email where the identity of the sender is disguised or concealed, as well as where there is no valid means of contact to send a request to stop these communications or encouraging recipients to visit websites that violate these rules is strictly forbidden.

ONLINE PRIVACY

Cookie compliance

As determined by Law 41/2004, of 18 August, storage of data and the possibility of accessing data stored in a subscriber or user terminal is only allowed if the subscriber or user has provided prior consent. Such consent must be based on clear and comprehensive information.

This does not prevent technical storage or access for the sole purpose transmitting communications over an electronic communication network, if strictly necessary for the provision of a service expressly requested by the subscriber or user.

Traffic Data

Traffic data must be erased or anonymized when no longer needed for the transmission of communications. Processing of traffic data requires prior express consent and the user or subscriber shall be given the possibility to remove it at any time. Such processing may only be carried out to the extent and for the time strictly necessary for the sale of electronic communications services or the provision of other value-added services.

Processing of traffic data is admissible when required for billing and payment and only until the end of the period during which the bill may lawfully be challenged or payment pursued.

Complete and accurate information on the type of data being processed must be provided, as well as the processing purposes and duration and the possibility of disclosure to third parties for the provision of value added services. Processing should be limited to workers or employees in charge of billing or traffic management, customer inquiries, fraud detection, sale of electronic communications services accessible to the public, or the provision of value added services, as well as to the strictly necessary information for the purposes of carrying out such activities.

Location Data

Processing of location data is allowed only if such data is anonymized or to the extent and for the time necessary for the provision of value added services, provided that prior express consent was obtained. Prior information to the data subjects must also be provided.

Companies must ensure there is an option to withdraw consent at any time, or to temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication, in a simple manner and free of charge.
Non-compliance with these opt-in rules is considered an administrative offence, punishable with fines ranging from EUR 5,000 to EUR 5,000,000.

KEY CONTACTS

Joao Costa Quinta
Partner
T +351 213 583 620
Joao.Quinta@pt.dlapiper.com

Margarida Leitão Nogueira
Partner
T +351 213 583 620
margarida.nogueira@pt.dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

QATAR

Last modified 17 January 2024

LAW

Note: Please also see Qatar Financial Center (a business center located on-shore in Qatar with its own regulations separate from those of the State of Qatar, including separate data protection regulations).

This overview is based on an unofficial English translation of the Law No. (13) of 2016 Concerning Personal Data Protection. The Qatar government does not issue official English translations of the laws of the State of Qatar.

Qatar has implemented Law No. (13) of 2016 Concerning Personal Data Protection ("**the Data Protection Law**").

With its Data Protection Law – adopted in 2016 – Qatar became the first Gulf Cooperation Council (GCC) member state to issue a generally applicable data protection law.

The Data Protection Law is supplemented with a set of regulatory guidelines issued by the National Cyber Governance and Assurance Affairs (NCGAA) of the National Cyber Security Agency. The guidelines incorporate concepts from EU privacy regulatory frameworks and seek to clarify obligations under, and address matters that are not dealt with in, the Data Protection Law. The introduction of these guidelines provide a mechanism for which those subject to the Data Protection Law would be able to better understand their obligations under the Data Protection Law and comply with its provisions more fully.

The Data Protection Law applies to personal data when this data is any of the following:

- Processed electronically;
- Obtained, collected or extracted in any other way in preparation for electronic processing; and
- Processed by combining electronic processing and traditional processing.

The Data Protection Law provides that each individual shall have the right to privacy of their personal data. Such data may only be processed within a framework of transparency, honesty, respect for human dignity and in accordance with the provisions of the Data Protection Law.

DEFINITIONS

Definition of personal data

Personal data is defined under the Data Protection Law as data relating to a natural person whose identity is identified or is reasonably identifiable, whether through this data or by means of combining this data with any other data or details.

Definition of sensitive personal data

Sensitive personal data means personal data consisting of information as to a natural person’s:

- Ethnic origin
- Health
- Physical or mental health or condition
- Religious beliefs
- Relationships
- Criminal records

NATIONAL DATA PROTECTION AUTHORITY

National Cyber Governance and Assurance Affairs (NCGAA) of the National Cyber Security Agency

REGISTRATION

There is currently no requirement in Qatar for data controllers who process personal information to register with the regulator, the NCGAA.

DATA PROTECTION OFFICERS

There is currently no obligation for organizations in Qatar to appoint a data protection officer. There is an obligation on the data controller to specify processors responsible for protecting personal data, train them appropriately on the protection of personal data and raise their awareness in relation to protecting personal data.

COLLECTION & PROCESSING

Generally, data subject consent is required to collect and process personal data, except to the extent processing is deemed necessary for a lawful purpose of the controller, or the third party to whom the personal data is sent.

Lawful purpose is defined in the Data Protection Law as "the purpose for which the personal data of the data subject is being processed in accordance with the law," which includes cases where a data controller is processing personal data for legitimate interests and specific purposes set forth under Data Protection Law as described below.

Prior to processing personal data, the data controller must notify the data subject of the following information:

- The details of the data controller or another party who processes the data on behalf of the data controller;
- The lawful purpose for which the data controller or any third party wants to process the personal data;
- A comprehensive and accurate description of the processing activities and the degrees of disclosure of personal data for the lawful purpose; and
- Any other information deemed necessary and required for the satisfaction of personal data processing.

The data controller is free to process data without the consent of the data subject or a lawful purpose in the following circumstances:

- The data processing is in the public interest. A data controller would process personal data in the public interest if it is conducting a specific task in the public interest pursuant to applicable law or is exercising "official authority" (e.g. a public body's tasks, functions or duties) pursuant to applicable law;
- The data processing is required to meet a legal obligation. A data controller would be considered processing personal data to meet a legal obligation where it is required to do so by virtue of the law or court order;
- The data processing is required to protect the data subject's vital interests. What constitutes as "vital interests" is applied very narrowly to cases of "life and death" and on the basis of humanitarian grounds such as in relation to a pandemic / epidemic. Further, this exemption is likely to arise in cases where data related health is being processed which is a category of sensitive personal data (explored further below) and in which case, this exemption would only apply if the data subject is physically or legally incapable of providing consent and as such, explicit consent may be more appropriate in the circumstances;

- The data processing is required for scientific research being conducted in the public interest. Cases involving the processing of personal data for "scientific research in the public interests" should be interpreted broadly and would include processing activities to further technological development or privately funded research; or
- The data processing is required to investigate a crime, if officially requested by the investigating authorities.

Sensitive personal data may not be processed except after obtaining authorization from the NCGAA. There is a high threshold for processing this data and, amongst other things, a data controller would be required to:

- Identify a permitted reason for processing sensitive personal data and an "additional condition" for processing activities and these "additional conditions" include, but are not limited to, (i) processing with the data subject's explicit consent or parental consent (as may be relevant), (ii) the personal data is made public by the data subject; or (iii) the processing is necessary in an employment context and would enable the data controller to fulfil their obligations as an employer;
- Complete a data protection impact assessment to identify, inter alia, the purpose and permitted reason for processing, the potential damage / harm that can be caused to the data subject as a result of the processing activities and the risks to the processing and methods / actions to mitigate such risks; and
- Obtain permission from the NCGAA to process such personal data which may be conditioned on, inter alia, the data controller evidencing to the NCGAAthat it has the appropriate administrative, technical and financial precautions in place to protect such special personal data.

TRANSFER

Data controllers may collect, process and transfer personal data when the data subject consents, unless deemed necessary for realizing a 'lawful purpose' for the controller or for the third party to whom the personal data is sent. The data controller has to demonstrate, when disclosing and transferring personal data to the data processor, that the transfer is for a lawful purpose and that the transfer of data is made pursuant to the provisions of the Data Protection Law.

Data controllers should not take measures or adopt procedures that may curb trans-border data flow, unless processing such data violates the provisions of the Data Protection Law or will cause gross damage to the data subject. The Data Protection Law defines 'trans-border data flow' as accessing, viewing, retrieving, using or storing personal data without the constraints of state borders.

SECURITY

Data controllers must take appropriate technical and organizational measures to securely manage personal data.

The data controller must carry out the following procedures:

- Review privacy protection procedures before implementing new processing operations
- Specify the processors responsible for protecting the personal data
- Train processors on the protection of personal data and raise their awareness relating to the same
- Set up internal systems to receive and investigate complaints, data access requests, data correction or deletion requests and provide the data subjects with information relating to the same
- Set up internal systems for the effective management of personal data, and report any violation of the same with the aim of safeguarding personal data
- Adopt suitable technical means to enable individuals to exercise their rights to access, review and correct their personal data directly
- Carry out comprehensive review and checking of the commitment to protect personal data
- Verify that the data processor abides by the instructions given to him/her or take suitable precautions to protect personal data, and continually monitor that situation

The data controller and processor must take necessary precautions to protect personal data against loss, damage, amendment, disclosure or access thereto or use thereof in an accidental or unlawful way. The Data Protection Law states the precautions taken must be proportionate to the nature and importance of the personal data to be protected. Organizations should adopt best practice methodologies in keeping with their business sector.

BREACH NOTIFICATION

There is an obligation on the data controller to notify the regulator, the NCGAA and the data subject of any breaches of the measures to protect the data subject's privacy if it is likely to cause damage to the data subject. The notification to the NCGAA and the data subject must be made as soon as possible from the time the data controller becomes aware of the breach but in any event, within 72 hours.

A personal data breach means a breach of security leading to an unlawful or accidental alteration, destruction, loss, unauthorised disclosure of, or access to personal data. This would encompass both, accidental and deliberate breaches such as, theft or loss of IT equipment, inadequate disposal of confidential files that may contain personal data material and using client data for a personal gain. In assessing whether a breach would cause serious damage, the data controller should take into consideration whether the breach would cause the data subject to be impacted negatively in various ways such as emotional distress, or physical or material damage.

ENFORCEMENT

In Qatar, the NCGAA is responsible for the enforcement of the Data Protection Law. Any data subject may submit a complaint to the NCGAA in the case of a violation of the Data Protection Law. The NCGAA will investigate the complaint and, if the complaint is found to be valid, the NCGAA can oblige the data controller or processor to rectify the violation within a specified time period.

The NCGAA can also impose fines of up to 5 million (US$1.4 million) for violations of the Data Protection Law.

ELECTRONIC MARKETING

Unsolicited direct marketing is prohibited under the Data Protection Law, which requires prior consent to send electronic marketing communications (including by wired or wireless communication). The consent of the data subject must be affirmative, explicit and unambiguous. Indirect or implied consent by means of pre-ticked boxes may be deemed invalid.

All electronic marketing communications must include the identity of the sender and an indication that it is sent for the purpose of direct marketing. The message must include an address that can easily be reached and must enable the recipient to send a message requesting the sender to stop the electronic communication and enable the recipient to withdraw the consent at any time.

ONLINE PRIVACY

The Data Protection Law specifically regulates online privacy processing data in relation to children. Owners and operators of websites must observe the followings requirements.

In relation to online privacy, data controllers must ensure they have in place a privacy notice to notify data subjects that they are processing personal data. A privacy notice must generally include the following information:

- Details of the data controller including its legal name, registered address and contact information
- Details regarding third-party processors if any and in which case, the privacy notice should, inter alia, provide a description of why the data processors are processing information on behalf of the data controller
- The data controller's purposes for processing personal data including the permitted reasons for doing so
- A comprehensive and accurate description of the processing activities
- The levels of disclosure for the permitted reasons for processing personal data or a general description
- Any other information that is necessary for fulfilling conditions of personal data processing for e.g., general information on how personal data is kept secure and a data subject's rights and how they may be exercised

In relation to websites relating to children, a data controller should:

- Place a notification on the website regarding how children’s data is used and its disclosure policies
- Obtain express approval from the parents or guardian of the child before processing any personal data

- Provide the child’s parent or guardian—upon request and after verifying the identity of the child’s parent or guardian—a description of the personal data that is being processed, stating the purpose of the processing, and a copy of the child’s data that is being collected and processed
- Delete, erase, or suspend the processing of any personal data that was collected from the child or about the child, if the child’s parent or guardian requests this, and
- Refrain from making any child's participation in a game or prize offer, or any other activity conditional on the child's submission of personal data which goes beyond what is required for the purposes of participation in the game or prize offer

KEY CONTACTS

Brenda Hill
Legal Director
T +974 4420 6126
brenda.hill@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

QATAR - FINANCIAL CENTRE

Last modified 17 January 2024

LAW

Note: Please also see Qatar.

The Qatar Financial Centre ("**QFC**"), a business center located on-shore in Qatar with its own regulations that are separate and distinct from those of the State of Qatar, implemented QFC Regulation No. 6 of 2005 on QFC Data Protection Regulations ("**DPL**").

Additionally, under the powers granted to the QFC Authority under Article 32(6) of the DPL, the QFC Authority has issued the Data Protection Rules 2005 (DPR).

The QFC updated the DPL and DPR on 6 December 2023. This note reflects the position under the DPL and DPR as amended. As a general comment, the changes provide increased clarity around the DPL and DRP as well as creating certain new obligations and bring the QFC more closely in line with the position under the GDPR and other similar laws, which should assist international businesses in taking a relatively uniform approach to their data compliance activities.

The DPL and DPR apply to the processing of personal data of living natural persons. Such processing may be by automated means or non-automated means. The DPL and DPR apply to data controllers and processors incorporated or registered in the QFC and to those that are not if, as part of ongoing arrangements, the data controller or processor process personal data through a data controller or processor that is incorporated or registered in the QFC unless it does so on an occasional basis.

DEFINITIONS

Definition of data controller

An individual or entity that determines the purposes and means of the processing of personal data.

Definition of data processor

An individual or entity that undertakes the processing of personal data on behalf of a data controller or another data processor.

Definition of data subject

A natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the data subject.

Definition of personal data

Any information relating to a data subject.

Definition of personal data breach

Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosed of, or access to, personal data transmitted, stored or otherwise processed.

Definition of processing

Any operation or set of operations that is performed (whether or not by automatic means) on personal data or on sets of personal data, and includes collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consultation, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing and destroying the personal data.

Definition of sensitive personal data

Personal data revealing or relating to race or ethnicity, political affiliation or opinions, religious or philosophical beliefs, trade-union or organizational membership, criminal records, health or sex life, and genetic and biometric data used to identify an individual.

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Office at the QFC Authority is the administrator of the DPL and DPR in the QFC ("**DPO**").

REGISTRATION

Unless certain exceptions apply, data controllers must obtain a permit from the DPO prior to processing sensitive personal data or transferring personal data outside of the QFC to a recipient who is not subject to laws or regulations that ensure an adequate level of protection for that personal data.

DATA PROTECTION OFFICERS

There is no requirement under the DPL or the DPR for organizations to appoint a data protection officer. Though note the general obligation of a data controller to implement appropriate technical and organizational measures to protect personal data, as further detailed below (see Security). It is however recommended that organizations that operates on a large scale or carries out regular and systematic monitoring of individuals appoint an individual responsible for overseeing the data controller’s compliance with data protection requirements.

COLLECTION & PROCESSING

Conditions for Consent

Data controllers must be able to show that the data subject's consent complies with the DPL where they are using consent as a basis for their processing activities.

Consent by a data subject must be:

- Freely given;
- Specific;
- Informed; and
- Unambiguous.

Where consent is given in a document that also concerns other matters then the consent must be:

- Clearly distinguishable;

- Intelligible and easily accessible; and
- Use clear, unambiguous and plain language.

Processing personal data

Data controllers may process personal data when any of the following conditions are met:

- The data subject has given his / her consent to the processing of that personal data;
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with an obligation to which the data controller is subject to by law;
- Processing is necessary in order to protect the vital interests of the data subject or another individual;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the QFC Authority, the QFC Regulatory Authority, QFC Civil and Commercial Court, the QFC Regulatory Tribunal or a QFC Institution;
- Processing is necessary for the purposes of the legitimate interests of the data controller or another person to whom the personal data is disclosed, except where such interests are overridden by legitimate interests of the data subject which require the data to be protected.

Processing sensitive personal data

Data controllers may process sensitive personal data when any of the following conditions are met:

- The data subject has given his / her explicit written consent to the processing;
- Processing is necessary for the purposes of carrying out the obligations and the exercise of specific rights of the data controller or the data processor in the field of employment law;
- Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his / her consent;
- Processing is carried out by an insurance firm for the purposes of providing a life or health insurance policy;
- Processing is carried out by a non-for-profit body in the course of its legitimate activities with appropriate guarantees that the processing relates solely to the members or former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed to a third party without the consent of the data;
- Processing relates to personal data which is manifestly made public by the data subject;
- Processing is necessary to establish, pursue or defend a legal claim or when a court is acting in its judicial capacity;
- Processing is necessary for compliance with an obligation to which the data controller is subject to by law;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the QFC Authority, the QFC Regulatory Authority, QFC Civil and Commercial Court, the QFC Regulatory Tribunal or a QFC Institution;
- Processing is necessary for substantial public interest reasons that are proportionate to the aim or aims pursued, respect the principles relating to the processing of personal data and provide suitable and specific measures to safeguard the rights of the data subject;
- Processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where that personal data is processed by a health professional subject under national laws or regulations established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

TRANSFER

Data controllers may transfer personal data out of the QFC if the personal data is being transferred to a Recipient in a jurisdiction that the DPO has decided has laws and regulations that ensure an adequate level of protection for that personal data. The DPO has produced a list of jurisdictions which it deems to have such adequate levels of protection and may also take the following factors into consideration when assessing the adequacy of the level of protection ensured by laws and regulations to which the Recipient is subject to:

- The rule of law, the general respect for individual's rights and the ability of individuals to enforce their rights by administrative or judicial means;
- The access of public authorities to personal data;
- The existence of effective data protection regulations including on onward transfer of personal data to another jurisdiction;
- The existence and functioning of one or more independent supervisory authorities with adequate enforcement powers;
- International commitments and conventions binding on the jurisdiction and its membership of any multilateral or regional organizations;
- Decisions taken by other data protection authorities where their decisions take into consideration the same factors as those the DPO does.

In the absence of an adequate level of protection, data controllers may transfer personal data out of the QFC if any of the following are true:

- The data controller or data processor have appropriate adequate safeguards including enforceable rights and remedies for the data subjects which may be provided by a legally binding and enforceable arrangement between public authorities or a legally binding and enforceable agreement between parties which contain data protection clauses adopted by the DPO;
- The data subject has been informed of the risks of such transfer and has given his / her explicit consent to the proposed transfer;
- Transfer is necessary for the performance of a contract between the data subject and the data controller, or the implementation of pre-contractual measures taken in response to the data subject’s request;
- Transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party;
- Transfer is legally required for the purposes of the data controller's or data processor's compliance with a legal obligation;
- Transfer is necessary in order to protect the vital interests of the data subject;
- Transfer is necessary to perform a task carried out in the public interest or by any of the following authorities in the performs of their functions, the QFC Authority, the QFC Regulatory Authority, the QFC Civil and Commercial Court, the QFC Regulatory Tribunal or a QFC Institution;
- Transfer is necessary for the establishment, exercise or defense of a legal claim.

If none of the above are applicable, a data controller may transfer personal data out of the QFC only if:

- DPO has granted a permit for the transfer or the set of transfers and the data controller applies adequate safeguards with respect to the protection of this personal;
- The transfer is based on binding corporate rules that fulfil the requirements of the DPR and approved by the DPO or another internationally acceptable transfer mechanism approved by the DPO; or
- The transfer:
    - Is not repeating or not part of a repetitive course of transfers;
    - Concerns only a limited number of data subjects;
    - Does not contain sensitive personal data;
    - Is for the purposes of the legitimate interests of the data controller or third party to which the data is disclosed unless sch legitimate interests are overridden by those of the data subject; and
    - The data controller has completed a documented assessment of the circumstances surrounding the data transfer and has provided adequate safeguards with regard to the protection of the personal data.

SECURITY

Data controllers and processors must implement appropriate technical and organizational measures to ensure an appropriate level of security in the processing of personal data. These measures include, but are not limited to:

- The de-identification and / or encryption of the personal data;
- Ability to ensure continuing confidentiality, integrity, availability and resilience of processing systems and advances;
- Ability to restore availability of and access to the personal data in a timely manner if a physical or technical incident has occurred;

- A process for routinely testing, assessing and evaluation the effectiveness of the measures.

The measures implemented ought to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected and in particular, to protect such personal data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the personal data. In assessing what measures are appropriate, data controllers and processors can consider:

- Availability of technology;
- Costs of implementation;
- The processing activities; and
- The likelihood and severity of the risks to the rights and legitimate interests of individuals.

BREACH NOTIFICATION

There is a requirement under the DPL to inform the DPO of a Personal Data Breach. The notification must be made without undue delay and where possible, no later than 72 hours from the time the data controller is made aware of the breach.

The data controller must also consider notifying the data subjects affected of the breach and if the data controller determines that it will notify the data subjects then, it must notify them without undue delay after becoming aware of the breach and its notification:

- Must use clear and plain language;
- Must contain an explanation of the nature of the personal data breach;
- Must describe the consequences (or those that are likely) of the data breach; and
- Must contain a description of the measures taken or proposed to be taken by the data controller to address the breach and the measures to mitigate the effects of the breach.

The requirement to notify the DPO of a personal data breach does not apply if the breach is unlikely to result in a risk to the rights and legitimate interests of the data subjects.

ENFORCEMENT

In the QFC, the DPO oversees the enforcement of the DPL.

The DPO has, *inter alia*, the following powers:

- To order a data controller or processor to provide information that the DPO requires for the purposes of its performance of its duties;
- To carry out investigations and audits;
- To issue reprimands or orders to rectify infringements of the DPL and DPR;
- To order a data controller or processor to comply with the data subject's requests to exercise its rights under the DPL;
- To order a data controller or processor to carry out processing operations in a specified manner; and
- To impose penalties and such other corrective measures.

ELECTRONIC MARKETING

Immediately upon collecting personal data, the DPL requires data controllers to provide data subjects who they have collected personal data from, with, among other things, any further information to the extent necessary. This includes information on whether the personal data will be used for direct marketing purposes.

If the personal data has not been obtained from the data subject, the data controller or their representative must at the time of undertaking the recording of personal data or within a reasonable period no longer than 30 days after obtaining the personal data (taking into account the circumstances in which data are processed) – or if it is envisaged that the personal data will be disclosed to a third party, no later than when the personal data is first recorded or disclosed – provide the data subject with, among other things, information regarding whether the personal data will be used for direct marketing purposes.

A data subject has the right to object at any time to the processing of their personal data for direct marketing purposes. In which case, the personal data must no longer be processed for such purposes.

ONLINE PRIVACY

The DPL or DPR do not contain specific provisions relating to online privacy, however, the broad provisions detailed above are likely to apply. In addition, as Qatar criminal law applies in the QFC, the privacy principles laid out therein may apply (see Qatar).

KEY CONTACTS

Brenda Hill
Legal Director
T +974 4420 6126
brenda.hill@dlapiper.com

Elias Al-Far
Associate
T +974 4420 6125
elias.al-far@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

REPUBLIC OF CONGO

Last modified 23 February 2024

LAW

The protection of personal data is governed by the law on the protection of data with a personal character N° 29 - 2019 of 10 October 2019 and was published in the official journal on 7 November 2019 (the "**Law**"). The Law entered into force on the date of its approval (25 November 2020).

Beside the Law, there are several sectoral laws or decrees that contain data protection aspects (on cybersecurity, mobile telecommunications, etc.)

DEFINITIONS

Definition of Personal Data

Any information relating to a natural person identified or identifiable directly or indirectly, by reference to an identification number or identifiable on the basis of one or more elements specific to his / her physical, physiological, genetic, psychological, cultural, social or economic identity.

Definition of Sensitive Personal Data

Genetic data, data relating to minors, data relating to offences, criminal convictions or security measures, biometric data and, all personal data revealing ethnic origin, parentage, political opinions, religious or philosophical beliefs, trade union membership, gender, health and sex life.

NATIONAL DATA PROTECTION AUTHORITY

The Law provides for the creation of a national data protection Commission by a separate law. This Commission plays an important role in the Law and its application. However, we are not aware this Commission has been established.

REGISTRATION

The Law requires, save for some exceptions, that the processing of personal data must be notified to the Commission. The Commission provides a confirmation of receipt of the notification after which the entity that made the notification can start processing personal data. If some of the data or sensitive personal data and the processing is not prohibited, a prior authorisation is to be obtained from the Commission. The Commission renders a decision within two months after receipt of the request to process certain sensitive personal data.

DATA PROTECTION OFFICERS

A data protection officer (*délégué à la protection des données*) needs to be appointed when the data procession is done by:

- a public entity;
- the nature of the data processing because of its nature, purpose or nature require a regular and systematic follow-up; or
- when the data processing is on a large scale for particular data.

COLLECTION & PROCESSING

The collection and processing of personal data can only be carried out with the prior and explicit consent of the person concerned. Some exceptions apply when the processing is for valid legal reasons, in the public interest, for the performance of an agreement or to protect the fundamental rights of the person concerned.

TRANSFER

Cross-border transfer of personal data is only allowed if the receiving state offers a similar protection of personal data and the Commission is notified in advance of the intention to transfer data to a third country.

SECURITY

The Law provides for a detailed overview of security measures that must be taken by the processor of personal data in order to secure the personal data.

BREACH NOTIFICATION

The processor of personal data must in case of a breach of the security inform the Commission without delay and at the latest within 72 hours after it identified the breach.

Mandatory breach notification

It is mandatory to notify every breach to the Commission, however, the 72 hours deadline does not apply in case there is no risk for the rights of the persons concerned. The breach must still be notified, but it must be explained why the breach was notified more than 72 hours after the identification of the breach.

The persons concerned must also informed of the breach if it poses an important risk for its rights.

ENFORCEMENT

No known cases as far as we know. The Commission is not yet established.

Criminal sanctions apply as well as fines ranging from USD 1,800 to 180,000.

ELECTRONIC MARKETING

Regulated by separate law.

ONLINE PRIVACY

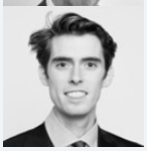
Regulated by separate law.

KEY CONTACTS

PKM Africa
www.lawpkm.com/

Yves Brosens
Partner
PKM Africa

T +32 472 582 000
yves.brosens@lawpkmafrica.com



Pierre Vanholsbeke
Junior Partner
PKM Africa
T + 32 472 79 54 24
pierre.vanholsbeke@lawpkmafrica.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ROMANIA

Last modified 17 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A regulation (unlike the directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An establishment may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extraterritorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "to the offering of goods or services" (no payment is required) to such data subjects in the EU or "the monitoring of their behaviour" as far as their behaviour takes place within the EU.

Law no. 190/2018 on the measures for the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("Law no. 190/2018") was published in the Official Gazette no. 651/26.07.2018 and became applicable on July 31, 2018.

Law no. 190/2018 regulates, among others, the following activities, in addition to providing certain derogations and a framework related to the sanctions applicable to public authorities and public bodies:

- Processing of genetic data, biometric data or health data
- Processing of a national identification number
- Processing of personal data in the context of employment relationships
- Processing of personal data and of special categories of personal data within the performance of a task carried out in the public interest

DEFINITIONS

Personal data is defined as "any information relating to an identified or identifiable natural person." A low bar is set for identifiable – if the natural person can be identified using “all means reasonably likely to be used” the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of **special categories** of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences.**

The GDPR is concerned with the **processing** of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a **controller** or a **processor**. The controller is the decision maker, the person who "alone or jointly with others, determines the purposes and means of the processing of personal data." The processor "processes personal data on behalf of the controller," acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The **data subject** is a living, natural person whose personal data are processed by either a controller or a processor.

Law no. 190/2018 does not provide any specific definitions with respect to personal data, as this term is already defined by the GDPR. However, the following relevant definitions are included:

- "Public authorities and bodies" means the Chamber of Deputies and the Senate, the Presidential Administration, the Government, the ministries, other specialized bodies of the central public administration, autonomous public authorities and institutions, local and county public administration authorities, other public authorities, as well as any institutions subordinated / coordinated by such authorities. Religious establishments, organisations and foundations of public service are considered public authorities / bodies.
- "National identification number" means the number by which an individual is identified in certain record systems and which has general applicability, such as: (i) personal identification number, (ii) serial number and identity card number, (iii) passport number, (iv) driving license, and (v) social health insurance number.
- "Remediation plan" means an annex to the report for finding and sanctioning misdemeanours, drafted by the National Supervisory Authority for Personal Data Processing (hereinafter referred to as ANSPDCP) setting remediation measures and terms.
- "Remediation measure" means a solution imposed by ANSPDCP in the remediation plan, in view of ensuring the compliance of the public authority/body with the obligations provided by the law.
- "Remediation term" means a time period of maximum 90 days calculated from the moment when the report for finding and sanctioning misdemeanours is communicated, in which the public authority/body may undertake remedial actions in order to correct any irregularities assessed by ANSPDCP and comply with its legal obligations.

All definitions included by the GDPR in Article 4 are applicable and have the same meaning as in Law no. 190/2018.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (similar to the CNIL in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the GDPR.

The GDPR creates the concept of "**lead supervisory authority**." Where there is cross-border processing of personal data (*ie* , processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single

establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by, and answer to, the supervisory authority for their main or single establishment, the so-called "lead supervisory authority."

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory. ead supervisory authority is therefore of somewhat limited use to multinationals.

The National Supervisory Authority For Personal Data Processing
(in Romanian 'Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal' or 'ANSPDCP')
28 30 Magheru Blvd
District 1, Bucharest
T +40 318 059 211
F +40 318 059 602
www.dataprotection.ro

REGISTRATION

There are no EU-wide systems of registration or notification, and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (*eg*, processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority.

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities, which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

All obligations in respect of notifying ANSPDCP of the processing of personal data were repealed on May 25, 2018 (when GDPR came into force).

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer (DPO) if it satisfies one or more of the following tests:

- It is a public authority
- Its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale
- Its core activities consist of processing sensitive personal data on a large scale

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities, provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have *expert knowledge* of data protection law and practices, though it is possible to outsource the DPO role to a service provider.

Controllers and processors are required to ensure that the DPO is involved "properly and in a timely manner in all issues which relate to the protection of personal data," and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks.

The specific tasks of the DPO, set out in GDPR, include:

- To inform and advise on compliance with GDPR and other Union and Member State data protection laws
- To monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff
- To advise and monitor data protection impact assessments where requested
- To cooperate and act as point of contact with the supervisory authority

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

In addition to the requirements provided by the GDPR in Articles 37 to 39, Law no. 190/2018 provides that a data protection officer (DPO) must be designated whenever the entity acting as controller is processing a national identification number, including by collecting or disclosing any documents enclosing such national identification number, when the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, in accordance with the provisions of Article 6 paragraph 1 letter (f) of the GDPR.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be:

- Processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle")
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle")
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- Accurate and where necessary kept up to date (the "accuracy principle")
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle")
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle")

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance for potentially years after a particular decision relating to processing personal data was rendered. Record-keeping, auditing and appropriate governance will all play a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "freely given, specific, informed and unambiguous," and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract

- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited, except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law.

Processing for a Secondary Purpose

Increasingly, organisations wish to re-purpose personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected. These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)

- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymisation

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, that is, the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language.

The following information must be provided at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten')

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (*eg*, commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling

Automated decision making (including profiling) "which produces legal effects concerning [the data subject] … or similarly significantly affects him or her" is only permitted where:

- Necessary for entering into or performing a contract
- Authorized by EU or Member State law
- The data subject has given their explicit (*ie*, opt-in) consent

Further, where significant automated decisions are taken on the basis of first or third grounds above, the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

1. Processing genetic data, biometric data or health data

The processing of genetic, biometric or health data for the purpose of achieving an automated decision-making process or for profiling purposes is permitted only with the explicit consent of the data subject or if the processing is performed based on express legal requirements, with the obligation to implement adequate measures for the protection of the rights, freedoms and legitimate interests of the data subject. Law no. 190/2018 does not specify or provide any examples with respect to what type of measures should be implemented in view of the processing.

Law no. 190/2018 expressly allows the processing of health data for the purpose of public health, as defined under Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work. However, subsequent processing of such data may not be performed for other purposes by third parties.

2. Processing a national identification number

Law no. 190/2018 provides that processing a national identification number, including by collecting or disclosing any documents enclosing such national identification number, may be carried out in the situations provided for in Article 6 (1) of the GDPR. However, where processing is based on the legitimate interests pursued by the controller or by a third party (i.e. Article 6 (1) (f) of the GDPR), the processing activities may be carried out only if the following guarantees have been implemented by the controller:

- Adequate technical and organizational measures to observe, in particular, the principle of data minimization and to ensure the security and confidentiality of personal data processing, according to the provisions of art. 32 of the GDPR;
- The appointment of a DPO;
- Establishment of retention terms in accordance with the nature of the personal data and the purpose of the processing, as well as specific deadlines in which personal data must be deleted or revised in order to be deleted;
- Regular training of the personnel processing personal data under the direct authority of the controller or processor.

3. Processing personal data in the context of employment relationships

The electronic monitoring and / or video surveillance systems of employees at the workplace based on the legitimate interests of the employer is / are permitted only if the following apply:

- The legitimate interests pursued by the employer are thoroughly justified and prevail over the interests or rights and freedoms of the data subjects;
- The employer has made the compulsory, complete and explicit prior information to the employees;
- The employer consulted the relevant trade union or, where applicable, the employees' representatives prior to the introduction of the monitoring systems;
- Other less intrusive forms and ways to achieve the goal pursued by the employer have not previously proved their effectiveness;
- The retention duration of personal data is proportional to the purpose of processing, but not more than 30 days, except for situations expressly governed by law or in duly justified cases.

4. Processing of personal data for journalistic purposes or for the purpose of academic, artistic or literary expression

According to Law no. 190/2018, in view of ensuring a balance between the right to personal data protection, freedom of expression and the right to information, processing of personal data for journalistic purposes, or for the purposes of academic, artistic or literary expression may be performed if such processing refers to personal data which were manifestly made public by the data subject or which are strongly connected to the quality of public person of the data subject or to the public nature of the facts in which the data subject is involved, by derogation from the following chapters of the GDPR:

1. Chapter II – Principles
2. Chapter III – Rights of the data subject
3. Chapter IV – Controller and processor
4. Chapter V – Transfers of personal data to third countries or international organizations

5. Chapter VI – Independent supervisory authorities
6. Chapter VII – Cooperation and consistency
7. Chapter IX – Provisions relating to specific processing situations

5. Processing of personal data for scientific or historical research purposes, statistical purposes or archiving in the public interest purposes

According to Law no. 190/2018 Articles 15, 16, 18 and 21 of the GDPR do not apply in case personal data are processed for scientific or historical research purposes or statistical purposes, to the extent the rights mentioned in these Articles are likely to render impossible or seriously impair the achievement of the objectives of the processing, and such derogations are necessary for achieving such objectives. These derogations are applied only with respect to archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and not with respect to other purposes for which the personal data may be used. Articles 15, 16, 18, 19, 20 and 21 GDPR do not apply in cases where personal data is processed for archiving purposes in the public interest to the extent that the rights mentioned in those Articles are likely to render impossible or seriously impair the achievement of the objectives of the processing, and such derogations are necessary for achieving such objectives. These derogations are applicable only with respect to scientific or historical research purposes and for archiving in the public interest purposes, and not with respect to other purposes for which the personal data may be used. Both these derogations are applicable only if appropriate safeguards for the rights and freedoms of data subjects are implemented, in accordance with Article 89(1) GDPR.

6. Processing of personal data and special categories of personal data by political parties, national minorities organisations and non-governmental organisations for the purpose of fulfilling their objectives

Processing of personal data and special categories of personal data by political parties, national minorities organisations and non-governmental organisations for the purpose of fulfilling their objectives can be done without the explicit consent of the personal data but with the application of the following:

- The information of data subjects on the processing of personal data;
- Guaranteeing the transparency of the information, of the communications and of the manner in which data subjects can exercise their rights;
- Guaranteeing the right to rectification and the right to erasure.

TRANSFER

Transfers of personal data by a controller or a processor to countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted when certain conditions are met.

The European Commission has the power to make an adequacy decision in respect of non-EU countries, determining that it provides for an adequate level of data protection, and thereby permitting personal data to be freely transferred to that country. Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes, among other things, binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where any of the following apply:

- Explicit informed consent has been obtained

- The transfer is necessary for the performance of a contract or the implementation of pre-contractual measures
- The transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person
- The transfer is necessary for important reasons of public interest
- The transfer is necessary for the establishment, exercise or defence of legal claims
- The transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained
- The transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject. Notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

No specific provisions / derogations are provided by Law no. 190/2018 with respect to personal data transfers.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

The GDPR does not prescribe specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A one-size-fits-all approach is therefore the antithesis of this requirement.

However, the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

- The pseudonymization and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

No specific provisions / derogations are provided by Law no. 190/2018 with respect to the security measures to be undertaken by controllers / processors.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay.

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach.

The notification to the supervisory authority must include where possible:

- The categories and approximate numbers of individuals and records concerned
- The name of the organisation’s data protection officer or other contact
- The likely consequences of the breach and the measures taken to mitigate harm

Controllers are also required to keep a record of all data breaches (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

No specific provisions / derogations are provided by the Law no. 190/2018 with respect to the notification of a personal data security breach. However, where data controllers notify a personal data breach to ANSPDCP, a special notification form must be filled out and submitted.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or €20 million (whichever is higher).

The European Commission intends that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that undertaking should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define undertaking and the case law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinized carefully to understand the interpretation of undertaking. Under EU competition law case law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on subsidiaries in some circumstances (broadly where there is participation or control), under a theory so-called look through liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories. The highest fines of up to €20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of any of the following:

- The basic principles for processing including conditions for consent
- Data subjects’ rights
- International transfer restrictions
- Any obligations imposed by Member State law for special cases such as processing employee data

- Certain orders of a supervisory authority

The lower category of fines of up to €10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of any of the following:

- Obligations of controllers and processors, including security and data breach notification obligations
- Obligations of certification bodies
- Obligations of a monitoring body

Supervisory authorities are not required to impose fines, but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive.

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered material or non-material damage as a result of a breach of the GDPR has the right to receive compensation from the controller or processor. The inclusion of non-material damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf.

Individuals also enjoy the right to lodge a complaint with a supervisory authority.

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision.

Data subjects enjoy the right to an effective legal remedy against a controller or processor.

ANSPDCP is entitled to investigate any breach of the GDPR provisions *ex officio* or following a complaint filed by a prejudiced data subject. The procedure on how ANSPDCP investigations can be conducted is provided by ANSPDCP Decision no. 161/2018.

Law no. 190/2018 provides specific rules with respect to enforcement. Specifically, ANSPDCP may issue written warnings and apply fines.

Misdemeanours committed by public authorities / bodies can be sanctioned with a fine ranging between RON 10,000 (approx. EUR 2,100) to RON 200,000 (approx. EUR 42,000).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time.

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC ("ePrivacy Directive"), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced by references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The processing of personal data for electronic marketing purposes is regulated under Law no. 506/2004, on the processing of personal data in the electronic communications sector implementing Directive 2002/58/CE ("Law no. 506 /2004").

According to this law, it is forbidden to send commercial communications by using automatic call and communication systems that do not require the intervention of a human operator, by fax or by electronic mail or any other method employing publicly available electronic communications services, except where the subscriber or user of a publicly electronic communications service has expressly consented in advance to receive such communications.

However, in cases where a natural or legal person has directly obtained the email address of a client upon the sale or provision of a product or service, the natural or legal person may use the respective address for the purpose of sending commercial communications regarding similar products or services, provided that clients are clearly and expressly offered the possibility to oppose by way of an easily accessible and free-of-charge method, not only when the email address is collected but also with each commercial communication received, in a case where the customer has not initially objected.

ONLINE PRIVACY

The processing of traffic data, location data and the implementation of cookies is regulated under Law no. 506/2004.

Traffic data

Traffic data relating to subscribers and users processed and stored by the provider of a public electronic communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication, but no later than three years from the date of such a communication.

However, traffic data may be retained for the purpose of marketing the services offered to data subjects, or in view of the provision of value-added services, solely throughout the marketing period and provided that data subjects have previously consented to the processing of traffic data. Data subjects may withdraw such consent at any time. The provider of publicly available electronic communication services must inform data subjects in respect of the processed categories of traffic data, and the duration of processing, prior to obtaining their consent.

The processing of traffic data for billing purposes or the establishment of payment obligations for interconnection is permitted solely for a period of three years following the due date of the respective payment obligation. The provider of publicly available electronic communication services must inform data subjects in respect of the processed categories of traffic data and the duration of processing.

The processing of traffic data for the establishment of contractual obligations of the communication services subscribers, with payment in advance, is permitted solely for a period of three years following the date of the communication.

The processing of traffic data as mentioned above may be done only by persons acting under the authority of providers of public electronic communications networks or of publicly available electronic communications services for:

- Management of billing and traffic
- Dealing with enquiries of data subjects
- Prevention of fraud, or
- The provision of communication services or value added services,

and it is permitted only if it is necessary to fulfil such purpose.

Location data, other than traffic data

The processing of location data, other than traffic data is permitted when:

- Data is rendered anonymous
- Data subjects have explicitly and consented prior to such processing for the duration necessary for the performance of value added services, or
- The purpose of the value-added service is the unidirectional and nondifferentiated transmission of information towards users.

The provider of publicly available electronic communications services must inform the users or subscribers, prior to obtaining their consent, in respect of the type of location data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent at any time. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the provider of publicly available electronic communications services must grant users the possibility, using a simple and free of charge means, of withdrawing consent or of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

Cookies

The storing of cookies on user terminals is permitted, subject to the following cumulative conditions:

- Subscribers or users have expressly consented thereto (Law no. 506/2004 also provides that consent may be given by way of browser settings or other similar technologies)
- The information requirements provided by Data Protection Law have been complied with in a clear and user-friendly manner, to include references regarding the purpose of processing of the information stored by users.

Should the service provider allow the storing of third-party cookies within a user's computer terminal, the user will have to be informed about the purpose of such processing and the manner in which browser settings may be adjusted in order to refuse third-party cookies.

Consent is not required where cookies are:

- Used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or
- Strictly necessary for the provision of an information service expressly requested by the subscriber or the user.

Failure to comply with the requirements of Law no. 506/2004 is classified as a minor offence and is sanctionable with fines ranging from approx. EUR 1,000 to EUR 21,000 . In the case of companies whose turnover exceeds approximately EUR 1.05 million, the amount of fines may reach up to 2% of the respective company's turnover.

Upon request of the courts of law, of the criminal prosecution authorities or of the authorities competent in the area of national defence and security with the prior approval of the judge, providers of publicly available electronic communication services and providers of public electronic communications networks shall make available, as soon as possible, but no later than 48 hours, traffic data, data regarding user terminals, as well as geolocation data.

KEY CONTACTS

Corina Badiceanu
Managing Associate
T +40 372 155 853
corina.badiceanu@dlapiper.com

Andrei Stoica
Junior Associate
T +40 372 155 870
andrei.stoica@dlapiper.com

Irina Macovei
Counsel
T +40 732 222 109
irina.macovei@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

RUSSIA

Last modified 17 January 2024

LAW

Fundamental provisions of data protection law in Russia can be found in the Russian Constitution, international treaties and specific laws.

Key legislation includes (but is not limited to):

- Federal law No. 152 FZ of 27 July 2006, “On Personal Data” (the Data Protection Act or DPA);
- Federal law No. 149-FZ of 14 July 2006, “On Information, Information Technologies and Protection of Information” (the Information Law); The Labor Code of the Russian Federation; and The Constitution of the Russian Federation.

The DPA is the most comprehensive source for Russia data protection rules and contains most of the provisions setting forth most of the provisions discussed herein. The Information Law sets forth rules related to information in a broader context and the Constitution provides for even broader rights to privacy (Articles 23 and 24). The Labor Code contains specific provisions for data protection in employment relationships.

Russia is a member of the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the Convention) (ratified by Russia in 2006).

DEFINITIONS

Definition of personal data

Personal data is defined in law as any information which relates directly or indirectly to a specific or defined physical person (the data subject). This can be widely interpreted in various contexts, so it is important to consider each situation carefully.

Definition of sensitive personal data

Sensitive personal data is defined as special categories of personal data in Russian legislation. Such special categories include data related to race, national identity, political opinions, religious and philosophical beliefs, health state, intimacies. While not specifically included as “sensitive” personal data, there are special rules for handling criminal records, so this should also be considered as sensitive.

Definition of biometric personal data

Biometric personal data is defined as information on physiological and biological features of a person, on the basis of which it is possible to and is used to establish the data subject’s identity. The definition of biometric personal data requires the data operator’s use of the information to identify the data subject.

Definition of personal data authorized by the personal data subject for dissemination

Intended to capture circumstances where a data subject has provided information or has given authorization for the dissemination of information to the public (mainly online), Russian law features a defined type of personal data as "personal data authorized by the personal data subject for dissemination.” The focus of the definition is not so much on the nature of the personal data itself, but the data subject’s authorization for its dissemination.

Data Operator

Russian law does not distinguish between “data controllers” and “data processors” in nearly all circumstances. Instead, the reference is to “data operators”.

NATIONAL DATA PROTECTION AUTHORITY

Federal Service for Supervision of Communications, Information Technologies and Mass Media or, in short, *Roscomnadzor* (‘Agency’)

Build. 2, 7, Kitaigorodskiy proezd
Moscow, 109074

Telephone

+7 495 987 6800

Fax

+7 495 987 6801

Website

rsoc.ru/

REGISTRATION

Russian law requires all data operators to notify the data regulator in writing about its intention to process personal data, unless very few narrow exclusions apply. The Federal Service for Supervision of Communications, Information Technology and Mass Media or “*Roskomnadzor*” (the Agency) is the data regulator for Russia.

The notification is made in a letter format and should contain the following information:

- the name and address of the data operator;
- the purpose of the processing;
- the measures of protection of personal data;
- name and contact information of the physical person or legal entity responsible for personal data processing;
- the data processing commencement date;
- information on occurrence or absence of cross border transfer of personal data;
- the term of processing or the conditions for termination of processing the personal data;
- information on personal data security provision;
- information on location of the database containing personal data of Russian citizens; and
- the name of the person or legal entity having access to and (or) carrying out the processing of personal data (based upon a contract) contained in state and municipal information systems.

DATA PROTECTION OFFICERS

If the data controller is a legal entity, it is required to appoint a data protection officer. Such an appointment is considered to be a personal data protection measure. The data protection officer oversees compliance by the data controller and its employees

regarding the data protection issues, informs them of statutory requirements and organises the receiving and processing of communications from data subjects.

There are no legal restrictions as to whether the data protection officer should be a citizen or resident of the Russian Federation, however, it is adviseable that the data protection officer is available in case there is an inspection or other communication from the authorities.

Non-appointment or improper appointment of the data protection officer is a violation of the data protection regime and may result in the imposition of penalties and enforcement protocols, as described below.

COLLECTION & PROCESSING

Data operators may collect and process personal data where any of the following conditions are met:

- The data subject consents;
- The processing is required by law or under an international treaty;
- The processing is required for administration of justice, execution of a court order or any other statements of public officers to be executed;
- The processing is required for provision of state or municipal services;
- The data operator needs to process the data to perform or conclude a contract to which the data subject is a party, a beneficiary party or guarantor;
- The processing is carried out for statistical or scientific purposes (except where processing is used also for advertising purposes), provided that it is depersonalized;
- The processing protects the data subject’s vital interests and it is impossible to obtain the data subject’s consent;
- The processing is required for execution of the data operator’s or third parties’ rights or for purposes important for the community, provided the data subject’s rights are not infringed;
- The processing is carried out by a journalist or media organization as a part of its professional activities or for the purposes of scientific, literary or other creative activities, except if the processing would infringe upon the data subject’s rights;
- The personal data is subject to publication or mandatory disclosure under law; or
- The personal data that is processed by participants under the conditions set forth in an experimental regulatory regime (sometimes referred to as a “regulatory sandbox") in depersonalized form.

Consent by the data subject is by far the most common legal basis for data processing in Russia. In most cases, consent may be given in any form, but it must be in some tangible format, as the data operator bears the burden of proof to show that consent was given, so, it is important to keep careful records of consents.

In some cases, however, DPA requires an explicit written consent:

- where the personal data is allowed by the data subject for dissemination;
- where sensitive or biometrical data is processed;
- where a legally binding decision is made solely on the grounds of the automated processing of personal data; or
- where employee personal data is transferred to third parties.

Consent is deemed to have been given in writing where it is signed by hand or in electronic form with a digital signature.

Written consent (except personal data allowed by the personal data subject for dissemination – there are special rules for this) must contain the following information:

- The identity of the data subject, (which can be made by reference to residential address and passport details);
- Identification of a data representative (if any);
- The identity and address of the data operator or the entity that processes personal data on behalf of the data operator (if any);
- The purpose of the processing;

- The list of personal data which may be collected and processed;
- The authorized types of processing;
- The term for which the consent remains valid;
- Means for revocation of consent; and
- The data subject’s signature.

For personal data allowed by the personal data subject for dissemination there must be a separate form of consent containing following information:

- Full name of the data subject;
- Contact information for the data subject (telephone number, e-mail address or postal address);
- Information on the data operator, including name, registered address, taxpayer identification number, and state registration number (if known to the data subject);
- Information about the information resources of the data operator, through which the processing of the personal data and access to the data will be provided, including identification of the protocol (http or https), server (www), domain, the directory on the server and file name of the web page;
- Purpose(s) of personal data processing;
- Descriptions of the personal data for which the consent is given, including “standard” personal data, any special categories of personal data, and any biometric data;
- Categories and list of personal data, for which the data subject establishes conditions and prohibitions;
- Conditions under which the personal data may be transmitted by the operator only through its internal network, providing access to information only for strictly defined employees, or using information and telecommunication networks, or without transmitting the personal data (to be filled in at the request of the personal data subject);
- The period of validity of the consent.

Consent in any case may be revoked at any time.

A key feature of Russian personal data law involves what is often referred to as the “Data Localization Rule” instituted in 2015. The Data Localization Rule requires all data operators to store and process any personal data of Russian individuals within databases located in Russia (subject to few exceptions). The penalty for violation of this requirement is ultimately the blocking of websites involving unlawful handling of Russian personal data and fines up to ₽6 000 000 and up to ₽18 000 000 for repeated violations.

According to DPA, storing and processing of personal data of Russian individuals outside of Russia can still be compliant with the law as long as the primary (often interpreted as initial) storage and other processing activities prescribed by DPA is done in Russia. As one can imagine, compliance with the Data Localization Rule can be complicated for international data operators.

TRANSFER

According to recently adopted amendments to the law, prior to a transfer of personal data out of Russia, the data controller must notify Roskomnadzor on cross-border data transferring.

The law distinguishes between the countries that provide adequate protection of personal data and countries that do not provide adequate protection of personal data. This differentiation impacts the procedure of data transferring as commented below.

The fact that the recipient state ratified the Convention is sufficient ground to deem that the state provides adequate protection of personal data for the purposes of the DPA.

In addition to the above, the *Roskomnadzor* issued the Order No. 274 of 15 March 2013 '*On endorsement of the List of the Foreign States Which are Not Parties to the EC Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data*'. The Order contains the list of countries which are officially recognized by Russian authorities as 'ensuring adequate protection'. Apart from the Member States of the Convention, there are 23 so 'white-listed' states as of today.

In connection to both types of countries Roskomnadzor has the right to restrict cross-border transfers. For the countries which provide the adequate protection of personal data the controller must notify Roskomnadzor beforehand but may commence the

cross-border data transfer without waiting for Roskomnadzor’s express or tacit approval of the transfer (and has to discontinue such transferring if Roskomnadzor objects). For the countries which do not provide the adequate protection of personal data for the purposes of the DPA, the transfer to those countries is not permissible until Roskomnadzor issues the express or tacit approval within the statutory set timeframes.

SECURITY

Data controllers are required to take appropriate technical and organisational measures against unauthorised or unlawful processing and accidental loss, changing, blocking or destruction of, or damage to, personal data.

A recent special regulation sets forth certain measures that the data controller should undertake to ensure security of personal data, data systems, carriers of biometrical information and technologies.

BREACH NOTIFICATION

Under the recently adopted amendments, in case of establishing the fact of unlawful or occasional transfer or dissemination of personal data, that caused a violation of data subject rights, the data controller must:

- within 24 hours notify *Roskomnadzor* about:
  - the incident;
  - believed reasons that caused violation of data subject rights;
  - estimated harm inflicted to data subject rights;
  - measures taken to cure consequences of the incident; and
  - details of the contact person to communicate with *Roskomnadzor*.
- within 72 hours notify *Roskomnadzor* about the results of internal investigation of the incident as well as to provide the information on the parties, if any, whose actions caused the incident.

The above timeframes are very short that may cause significant practical difficulties in complying with them.

ENFORCEMENT

In Russia, the Agency is responsible for the enforcement of data protection rules. The Agency is entitled to:

- carry out checks;
- consider complaints from data subjects;
- demand necessary information about personal data processing by the data operator;
- order the data operator to undertake certain actions according to the law, including discontinuance of the processing of personal data;
- file court actions;
- initiate criminal cases; and
- impose administrative liability for violations of data privacy rules.

If the Agency becomes aware that a data operator is in violation of the law, an enforcement notice may be issued, requiring the data operator to correct the violation.

A data operator can face civil or administrative penalties for violation of personal data law. Executives of the data operator responsible for violation of data rules may also face personal liability, including, in some cases, criminal liability. Criminal liability is not often applied, but may be imposed for violations, such as:

- Unlawful collection or dissemination of information about a data subject's private life, personal or family secreta, or public dissemination or leak to mass media of such information;
- Violation of data subjects’ right so secrecy of correspondence, telephone conversations, postal, telegraphic and other communications; or

- Unlawfully accessing legally protected computer information, if this act resulted in the destruction, blocking, modification or copying of computer information, including personal data.

Usually, in the case of violation of data protection law, the Agency will serve an enforcement notice requiring the correction of the violation. In many cases, the Agency and may also impose an administrative penalty and in some cases, may also recommend further actions against the individuals responsible for the violation.

The default administrative fines for most initial violations of data privacy rules are between ₽60, 000 – 150, 000 and ₽300,000 for repeated violations.

There are some specific rules for a breach of rules for written consent. In these cases, the fine for initial offences is between ₽ 300, 000 and ₽700, 000, and for repeated violations ₽1, 000, 000 – ₽1, 500, 000.

For violation of data localization rules, the maximum administrative penalty is currently ₽18, 000, 000 for repeated violations, actual penalties are imposed at lower levels.

The State Duma is considering significantly increasing existing fines and implementing new fines:

- Failure to fulfill or untimely fulfillment of the obligation to notify the Agency of the intention to process personal data - from ₽ 100,000 to ₽300,000;
- Failure to notify or late notification of the Agency of a leak of personal data. Companies are proposed to be fined up to ₽3, 000, 000 for this violation;
- Actions (or inaction) of the data operator causing a leak of personal data would involve a fine for companies between ₽5, 000, 000 and ₽20, 000 000, depending upon the number of affected data subjects, as well as the number of identifiers relating to affected data subjects. For repeated leaks, a fine ranging from 0.1% to 3% of the data operator’s aggregate revenue (in any case it must be not less than ₽15, 000, 000 or more than ₽ 500, 000, 000); and
- It is also proposed to criminalize the unlawful processing of computer information containing personal data, as well as the creation or operation of information resources intended for the unlawful storage or dissemination of such information. Penalties would include fines, compulsory labor and imprisonment.

While there has been a strong negative reaction in industry to the new fines and it would be expected that the proposed bill will be changed, it does appear that higher penalties for data law violations will come into force in the foreseeable future.

ELECTRONIC MARKETING

Processing of personal data for directly contacting data subjects for purposes of sales and marketing is allowed only with the consent of the data subject. In addition to the consent requirement under personal data rules, electronic marketing activities are regulated by the Law “on Advertising” No. 38-FZ dated 13 March 2006. The Advertising Law features an Anti-Spam rule under which the distribution of advertising through telecommunications networks, in particular, through the use of telephone, facsimile and mobile telephone communications, is allowed only with the consent of party receiving the advertising. The advertiser bears the burden of proof to show that consent was received. Consent to receive advertising may be revoked at any time, and the advertiser is obligated to immediately cease distribution of the advertising upon such revocation.

ONLINE PRIVACY

Russian data law does not generally specifically regulate online privacy. That said, however, Russian personal data rules are broadly written so that they would apply to online privacy, and it would appear that online privacy was a concern of the legislators when the rules are drafted. One specific area of application of the rules to online privacy involves the specific rules for personal data subject for dissemination.

Personal data allowed by the personal data subject for dissemination

A certain subset of personal data involves that data for which a data subject has given consent for dissemination. While not specifically limited to online dissemination, these rules were made with online activity in mind – particularly social media

and other platforms from which information is shared. Consent in this regard must be executed separately from other consents of the subject of personal data to the processing of his / her personal data and requires specificity about the types of personal data which may be disseminated. The data operator must provide the data subject with the opportunity to determine the list of personal data for each category of personal data specified in the consent. The consent must be explicit; silence or inaction of the personal data subject can under no circumstances be considered as implied consent.

The data subject may establish prohibitions on the transfer or disclosure (except for granting access) of the personal data by the data operator, as well as prohibitions or conditions on public processing (except for obtaining access) of thee. The data operator must publish information on these prohibitions and conditions on processing within three working days from the date of obtaining the relevant consent of the data subject.

The data subject may revoke consent at any time. The transfer, dissemination, provision, or granting access to personal data authorized by the personal data subject for dissemination shall be stopped within three working days from the request of the data subject.

In case of public disclosure of personal data directly by the data subject, the personal data, although disclosed, is still protected under law. So, where a data subject makes the personal data public (for example on social media), further dissemination or processing of this personal data still must be performed under a valid legal basis (usually consent).

In cases of public disclosure of personal data was done unlawfully or under force majeure circumstances, that personal data is also still protected under law and the further dissemination or other processing of such personal data lies on each person who carried out the dissemination or other processing.

Cookies

There is a well-established approach that cookies may constitute personal data if the information contained fits the definition of personal data (pertaining to or able to be used to identify a data subject) and in such cases, there must be a consent for its processing. As most cookies do carry personal data, necessity for consent is, in practice, presumed.\

Other

In addition to cookies, other types of information associated with online activity may also constitute protected personal data. If information on number, length of visits of particular web-sites, IP address and other information relates directly or indirectly to a specific or defined physical person then that would constitute protected personal data. Information regarding online activity may also be governed by legal protections in additional personal data laws, for example, those involving secrecy of communications.

KEY CONTACTS

Michael Malloy
Partner
Nextons
T +7 812 325 84 44
michael.malloy@nextons.ru

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

RWANDA

Last modified 17 January 2024

LAW

The law governing data protection in Rwanda is the Law n°058/2021 of 13/10/2021 relating to the protection of personal data and privacy (the “**Data Protection Law**”).

Data Protection Law came into effect 15th October 2021. Data controllers and processors who are already in operation have a period of two (2) years from the Data Protection Law commencement date to conform to its provisions.

The Law n° 24/2016 of 18/06/2016 governing Information and Communication Technologies in Rwanda (the “**ICT Law** ”).

The Law n° 60/2018 of 22/8/2018 on prevention and punishment of cyber-crimes (the “**Cyber Crime Law**”).

DEFINITIONS

Definition of Personal Data

The Data Protection Law defines personal data as *“any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as:*

- *name*
- *identification number*
- *location data*
- *an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person”* (article 3, 1°).

Definition of Sensitive Personal Data

The Data Protection Law defines sensitive personal data as *“information revealing a person’s race, health status, criminal records, medical records, social origin, religious or philosophical beliefs, political opinion, genetic or biometric information, sexual life or family details”* (article 3, 2°).

NATIONAL DATA PROTECTION AUTHORITY

The supervisory authority regarding Data protection is the National Cyber Security Authority (“**NCSA**”) (article 3, 23°).

REGISTRATION

A Data Controller is defined as a *“natural person, public or private corporate body or legal entity which, alone or jointly with others, processes personal data and determines their means of their processing”* (article 3, 19 °).

A Data Processor is defined as a *“natural person, public or private corporate body or legal entity, which is authorised to process personal data on behalf of the data controller”* (article 3, 24°).

Data controllers (“**DC**”) and Data Processors (“**DP**”) are required to register with the NCSA. (article 29).

The registration application must indicate the following (article 30):

- identity of the DC or DP and their designated single point of contact;
- identity and address of their representative if they have nominated any;
- description of personal data to be processed and the category of data subjects;
- whether or not the applicant holds or is likely to hold the types of personal data based on the sectors in which it operates;
- purposes of the processing of personal data;
- categories of recipients to whom the DC or DP intends to disclose the personal data;
- country to which the applicant intends to directly or indirectly transfer the personal data; and
- risks in the processing of personal data and measures to prevent such risks and protect personal data.

The NCSA issues a DC or DP registration certificate within 30 days of the application.

A regulation from the NCSA determining the validity period of the registration certificate is yet to be adopted (article 31).

DATA PROTECTION OFFICERS

The Data Protection Law requires that the DC and DP designate a data protection officer in the following cases (article 40):

- the processing of personal data is carried out by public or private corporate body or a legal entity, except courts;
- the core activities of the DC or the DP consist of personal data processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale;
- the core activities of the DC or the DP consist of processing on a large scale of sensitive personal data and personal data of convicts in accordance with the Data Protection Law’s requirements for the process of such data.

COLLECTION & PROCESSING

The DC is required to only collect personal data for a lawful purpose connected to its the activity and when the data is necessary for that purpose (article 42).

When collecting personal data, the DC is required to inform the data subject of the following:

- identity and contact details;
- purposes for which personal data are collected;
- recipients of such personal data;
- whether the data subject had the right to provide personal data voluntarily or mandatorily;
- the existence of the right to withdraw consent at any time and that such withdrawal does not affect the lawfulness of the processing of personal data based on consent before its withdrawal;
- the existence of the right to request from the DC access and ratification, restriction or erasure of personal data concerning the data subject or to object to the processing of the data;
- the existence of automated decision-making including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such processing personal data for the data subject;
- the period for which personal data will be stored;
- the right to appeal to the supervisory authority;

- where applicable, that the DC can transfer personal data outside of Rwanda and assures the data subject of the personal data security;
- any further information likely to guarantee fair processing of the personal data, having regard to the specific circumstances in which the data are collected.

The DC is not subject to the above disclosure requirements if:

- the data subject already has the information;
- the provision of such information proves impossible or involves a disproportionate effort; or
- the recording or disclosure of the personal data is required by the Data Protection Law.

The DC or DP must handle personal data for lawful purposes which include the following (article 46):

- the data subject’s consent to process their personal data for purpose explained to them;
- processing is necessary:
    - for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
    - for the execution a legal obligation to which the DC is subject;
    - for the protection of vital interests of the data subject or any other person;
    - for the performance of a duty carried out in the public interests or in the exercise of official authority vested in the DC;
    - for the performance of duties of a public entity;
- the processing is intended for legitimate interests pursued by the DC or by a third party to whom the personal data are disclosed, unless the processing is unwarranted in any particular case having regard to the prejudice to the rights and freedoms or legitimate interests pursued by the data subject;
- the processing is carried out for research purposes upon authorization by relevant institution.

The Data Protection Law also provides for requirements relating to the processing of personal data of a child under the age of 16 years which include the following (article 9):

- processing of the child’s personal data is subject to obtaining the consent of the holder of parental responsibility over the child;
- the consent obtained on behalf of the child must be given in the child’s interest to be acceptable;
- the consent is not required if it is necessary for protecting the vital interest of the child.

The DC or DP must store personal data in Rwanda. Storage of personal data outside of Rwanda is only permitted if the DC or DP holds a valid registration certificate authorising them to transfer or store personal data outside Rwanda (article 50).

TRANSFER

The transfer of personal data outside of Rwanda is only permitted for the following cases (article 48):

- the DC or DP has obtained authorization from the NCSA after providing proof of appropriate safeguards with respect to the protection of personal data;
- the data subject has given his or her consent;
- the transfer is necessary:
    - for the performance of a contract between the data subject and the DC or the implementation of a pre-contractual measures taken in response to the data subject’s request;
    - for the performance of a contract concluded in the interest of the data subject between the DC and a third party;
    - for public interest grounds;
    - for the establishment, exercise, or defense of a legal claim;
    - to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving his or her consent;
    - for the purpose of compelling legitimate interests pursued by the DC or by the DP, which are not overridden by the interests, rights and freedoms of the data subject and when:

    - transfer is not repetitive and concerns only a limited number of data subjects;
    - the data controller or the data processor has assessed all the circumstances surrounding the data transfer and has, on the basis of that assessment, provided suitable safeguards with regard to the protection of personal data;
  - for the performance of international instruments ratified by Rwanda.

The DC or DP transferring personal data outside of Rwanda must enter into a written contract with the transferee setting out the respective roles and responsibilities of each party to ensure compliance with the Data Protection Law (article 49).

A regulation from the NCSA determining the form of contract to be used for transfers of personal data outside Rwanda is yet to be adopted (article 49).

SECURITY

The DC and DP are required to ensure security of the personal data in their possession by adopting appropriate, reasonable technical measures to prevent loss, damage or destruction of personal data which include the following (article 47):

- identify foreseeable risks to personal data under that person’s possession or control, establish and maintain appropriate safeguards against those risks;
- regularly verify whether the personal data safeguards are effectively implemented;
- ensure that the personal data security safeguards are continually updated in response to new risks or any identified deficiencies.

The NCSA is entitled by the Data Protection Law to conduct inspection and assessment of these security measures.

The Data Protection Law also provides for safeguards that DC or DP processing sensitive personal data must adopt including storing sensitive personal data separately from other types of data or applying measures such as tokenisation, pseudonymisation or encryption (article 11).

BREACH NOTIFICATION

In case of personal data breach, the DC is required to communicate the personal data breach to the NCSA within 48h after being aware of the incident. The DP is required to notify the DC of any personal data breach within 48h after being aware of the incident (article 43).

Where the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject, the DC is also required to communicates the personal data breach to the data subject in writing or electronically, after having become aware of it (article 45). The Data Protection Law does not specify in which delay this communication must be done.

This communication of personal data breach to the data subject is not required in the following cases:

- the DC has implemented appropriate technical and organisational protection measures in relation to personal data breached such that the personal data breach is unlikely to result in a high risk to the rights and freedoms of the data subject;
- the DC has taken measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialize;
- the DC communicated it to the public whereby the data subject is informed in an equally effective manner.

The NCSA can request the DC to make such communication if the DC has not done it yet in case the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject.

ENFORCEMENT

The Data Protection Law provides for administrative misconduct sanctioned by administrative fines (article 53) and offences sanctioned by imprisonment and fines (article 56 to 63).

The administrative fines related to administrative misconduct imposed by the NCSA include operating without a registration certificate, failure to designate a personal data officer, failure to respect obligations related to personal data breach (notification, report, and communication) (article 53). The administrative fine is between RWF 2,000,000 to RWF 5,000,000 or 1% of the global turnover of the preceding financial year for corporate body or legal entity.

Any person not satisfied with the administrative sanction taken against them has the right to file an application to the competent court (article 54).

The NCSA is the initial organ in charge of settlement of conflicts arising in relation to the Data Protection Law.

The Data Protection Law provides that the following violations are considered criminal offences (article 56 to 61):

- access, collection, use, offer, share, transfer or disclosure of personal data contrary to the Data Protection Law;
- re-identification of de-identified personal data contrary to the Data Protection Law;
- destruction, erasure, concealment or alteration of personal data contrary to the Data Law Protection Law;
- sale of personal data contrary to the Data Protection Law;
- collection or process of sensitive personal data contrary to the Data Protection Law;
- provision of false information.

Corporate body or legal entity convicted of committing offence(s) is liable to a fine amounting to 5% of the annual turnover of the previous financial year (article 62).

Additional penalties for the offences that the court can order include (article 63):

- seizure or confiscation of items used in the commission of any of the offences;
- permanent or temporary closure of the legal entity or body or the premises in which any of the offences were committed.

ELECTRONIC MARKETING

The Data Protection Law provides for the data subject right to object to the processing of his/her personal data for direct marketing purposes including profiling to the extent that it is related to such direct marketing (article 19).

The ICT Law provides that a person who sends unsolicited commercial communications to a consumer, provides the consumer with the option to cancel the subscription to the mailing list of that person and identify particulars of the source from which that person obtained the consumer's personal information, upon the request of the consumer (article 168).

The ICT Law also provides that a person is not allowed to transmit, nor instigate the transmission of, a communication for the purposes of direct marketing by means of electronic mail where (article 223):

- the identity of the person who has sent the communication has been disguised or concealed;
- an address to which the recipient of the communication may send a request that such communication ceases has not been provided.

Sending unsolicited commercial communication to consumer is sanctioned by an administrative fine of between RWF 50,000 and RWF 500,000.

The Cyber Crime Law establishes spamming as a criminal offence (article 37). The Cyber Crime Law defines spamming as any intentional and without authorisation from a competent organ sending of unsolicited messages repeatedly or to a large number of persons by use of a computer or a computer system. Spamming also include the use of a computer or a computer system, after receiving a message, to retransmit such a message to many persons or retransmit it several times to a person who doesn’t need it.

The penalties for this offence are an imprisonment term of 3 months to 6 months and a fine of RWF 300,000 to RWF 500,000 (article 37).

The prosecution of spamming offence is however instituted only upon complaint of the offended person (article 37).

ONLINE PRIVACY

The Data Protection Law provides that the DC, DP or third-party processing personal data must respect the privacy of the data subject (article 5). It does not provide any other specific requirement regarding cookies and location data.

KEY CONTACTS

Moses Kiiza Gatama
Senior Partner
T +250 788 303 877
moses.kiiza@equityjuris.com

Ian Mulisa
Partner
T +250 788 678 515
ian.mulisa@equityjuris.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SAUDI ARABIA

Last modified 23 February 2024

LAW

The Personal Data Protection Law (issued pursuant to Royal Decree No. M/19 of 9/2/1443 H (corresponding to 16 September 2021), as amended by Royal Decree No. M/148 dated 5/9/1444H (corresponding to 27 March 2023)) ("**PDPL**") came into effect on 14 September 2023, but data controllers have a further year in which to comply (although that period may be further extended for certain entities). Accordingly, businesses within the scope of the PDPL will have until 14 September 2024 to adjust their status to become compliant with the PDPL.

The Implementing Regulations are also now in force, and provide further detail and guidance on various requirements in the PDPL. It comprises of two connected regulations, with the first being the 'Implementing Regulations to the PDPL', and the second being the 'Regulations on Personal Data Transfers outside the Kingdom' ("**Transfer Regulations**").

The PDPL is a law that applies on a national level and will apply to all sectors, with certain limited exceptions. For this reason, the PDPL will need to be considered in the broader legal and regulatory framework of the Kingdom of Saudi Arabia ("**KSA**"), with other sector specific frameworks such as those issued by the Saudi Central Bank, National Cybersecurity Authority or Communication, Space and Technology Commission ("**CST**").

DEFINITIONS

Definition of personal data

Personal data is defined as "*every data – of whatever source or form – that would lead to the identification of the individual specifically, or make it possible to identify him directly or indirectly, including: name, personal identification number, addresses, contact numbers, license numbers, records, personal property, bank account and credit card numbers, fixed or moving pictures of the individual, and other data of personal nature.*"

Definition of sensitive personal data

Sensitive data is defined as "*every personal data that includes a reference to an individual's ethnic or tribal origin, or religious, intellectual or political belief, or indicates his membership in nongovernmental associations or institutions, as well as criminal and security data, biometric data, genetic data, credit data, health data, location data, and data that indicates that both parents of an individual or one of them is unknown.*"

NATIONAL DATA PROTECTION AUTHORITY

The Saudi Authority for Data and Artificial Intelligence ("**SDAIA**") will be the data regulator for at least two years. During this time, consideration will be given to transferring the competence to supervise the application of the PDPL (and its Implementing Regulations) to the National Data Management Office.

The Saudi Central Bank and the CST both appear to maintain their jurisdiction to regulate data protection within their remit.

REGISTRATION

The PDPL has introduced a potential requirement for data controllers to register with SDAIA. It is expected that SDAIA will issue rules regarding such registration and will specify which data controllers must register.

DATA PROTECTION OFFICERS

The PDPL clarifies when a data controller must appoint a data protection officer. This includes where the data controller is a public entity that provides services involving the processing of personal data on a large scale, where the primary activities of the data controller consist of processing operations that require regular and continuous monitoring of individual also on a large scale, and where the core activities of the data controller consist of processing sensitive data.

COLLECTION & PROCESSING

The PDPL applies to any processing of personal data related to individuals that takes place in KSA by any means, including the processing of personal data related to individuals residing in KSA by any means by any entity outside KSA.

Under the PDPL, the primary legal basis for processing of personal data is consent of the data subject. However, the PDPL also provides for circumstances where consent is not required for processing of personal data.

TRANSFER

There are detailed rules relating to the transfer of personal data outside of KSA. The PDPL allows for the transfer of personal data outside of KSA for several purposes (for example, if such action is taken to meet an obligation to which the data subject is a party) and subject to various conditions (for example, the transfer or disclosure must not compromise the national security or vital interests of KSA and be limited to the minimum amount of personal data needed).

Subject to such requirements and conditions, the Transfer Regulations have introduced a number of circumstances where a cross border transfer of personal data is permissible. This includes to countries with appropriate levels of protection and no less than the protections afforded under the PDPL.

However, transfers of personal data to countries which are not deemed as having an adequate level of protection may still be made where "appropriate safeguards" are put in place. If the data controller is unable to use any of the appropriate safeguards, there are still limited cases where cross border transfers are permissible. Such transfers are still however subject to various controls.

In addition, in certain contexts or sectors, specific approvals may be required - for example, in a banking context, approval from the Saudi Central Bank.

SECURITY

Data controllers must take necessary organisational, administrative and technical measures and means to ensure personal data is preserved, including when it is transferred, in accordance with the provisions and controls specified in the Implementing Regulations.

BREACH NOTIFICATION

The PDPL imposes data breach notification requirements on data controllers, to notify the regulator (i.e. SDAIA) and / or impacted data subjects, depending on the circumstances. Where a notification is required to SDAIA, the data controller must notify within 72 hours of becoming aware of the breach. Where a notification is required to impacted data subjects, this must be made without undue delay.

In addition, notification obligations may be triggered in specific contexts / sectors – for example, cloud service providers may be required to report security breaches to the CST depending upon the circumstances.

ENFORCEMENT

Under the PDPL, the following penalties apply with respect to violations:

- Disclosure or publication of sensitive data in violation of the PDPL with intent to harm the data subject or to achieve a personal benefit, is punishable by imprisonment for up to two years and/or a fine up to SAR 3 million;
- For other breaches of the PDPL not covered by the previous point, this is punishable by a warning or by a fine not exceeding SAR 5 million. Separately, SDAIA has the power to issue warnings / administrative fines of up to SAR 5 million for any other violation, which is appealable. This is without prejudice to any more severe penalty stipulated in another law.

Note, the competent court may double the penalty of a fine for repeat offenders (even if this results in exceeding the maximum limit(s) set out above, provided that it does not exceed double the limit(s)).

Further, the competent courts may order confiscation of funds obtained as a result of committing violations (without prejudice to bona fide third party rights). The competent courts / committee may also order publication of a summary of the judgement or decision at the violator's expense.

Any person who suffers harm as a result of violation of the PDPL has a right to claim compensation before the competent court for material or moral damage.

ELECTRONIC MARKETING

There are specific rules in KSA relating to the use of personal data for marketing purposes. The PDPL and its Implementing Regulations contain various conditions around when personal data may be processed for the purposes of direct marketing. Additional requirements may also apply in certain contexts – for example, in the context of e-commerce activity.

ONLINE PRIVACY

There is no specific legislation in the KSA that specifically regulates the use of cookies.

KEY CONTACTS

Mohamed Moussallati
Legal Director
T +966 11 288 5449
mohamed.moussallati@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SENEGAL

Last modified 23 February 2024

LAW

The data protection regime in Senegal is mainly governed by the following laws and regulations:

- Act No 2008-12 of 25 January 2008 Concerning Personal Data Protection ("**the Act**");
- Decree No 2008-721 of 30 June 2008 on electronic certification in application of law no. 2008-08 of 25 January 2008 on electronic transactions.
- Act No. 2008-08 of January 25, 2008, on electronic transactions; and
- Act no. 2016-29 dated 8 November 2016 amending Law No.65-60 of 21 July 1965 on the Penal Code of Senegal.

As regards international conventions, Senegal is a member of the African Union Convention on Cyber Security and Protection of Personal Data known as the Malabo Convention adopted by the General Assembly of the African Union on 27 June 2014.

The aim is to create a comprehensive legal framework for e-commerce, data protection, cybercrime and cybersecurity on the continent.[1]

1: Christelle HOUETO, "Entry into force of the Malabo Convention on Cybersecurity in Africa: The countries".

DEFINITIONS

Definition of Personal Data

“Personal Data” means all data relating to an identified or identifiable individual by reference to an identification number or one, or many, characteristics of his / her physical, physiological, genetic, psychical cultural, social and economic identity.[1]

Definition of Sensitive Personal Data

“Sensitive Personal Data” means all data relating to religious, philosophical or political opinions or union activities; sex, life, race, health, social measures and prosecutions; and criminal and administrative sanctions.[2]

Definition of Electronic Trading

“Electronic Trading” means the act of offering, purchasing or supplying goods and services via computer systems and telecommunication networks such as the Internet or any other network using electronic, optical or other similar means enabling remote exchanges of information.[3]

Definition of Processing

“Processing [of Personal Data]” means any operation or set of operations which is performed upon data, whether or not by automatic means, such as collection, use, recording, organisation, storage, adaptation, alteration, retrieval, transmission, dissemination or otherwise making available, alignment or combination, blocking, encryption, erasure or destruction of personal data.

1: 2008-12 on the Protection of Personal Data; Article 4 Number 6

2: 2008-12 on the Protection of Personal Data; Article 4 Number 8

3: Article 1er of the African Union Convention on Cyber Security and Protection of Personal Data

NATIONAL DATA PROTECTION AUTHORITY

The authority responsible for data protection is the Senegalese Data Protection Authority established by Law No. 2008-12 of 25 January 2008.[1]

Commission for the Protection of Personal Data of Senegal (CDP) is located at 34 Sicap Mermoz VDN Lot B. 25528 Dakar, Fann.

The CDP is composed of eleven 11 members chosen because of their legal and / or technical competence. They:

- Ensure that the processing of character data is implemented in accordance with the legal provisions;
- Inform the data subjects and controllers of their rights and obligations;
- Regulate the assurance that information and communication technologies (ICTs) do not threaten the freedoms and privacy of Senegalese;
- Advise individuals and organizations who have used personal data processing or who have already undergone tests or experiences of a nature about such treatments;
- Publish the authorizations granted and the declaration issued to the directory of the processing of personal data and draw up an annual report of activities submitted to the President of the Republic and the President of the National Assembly.

The CDP also formulate recommendations by cooperating with the personal data protection authorities of third countries and participate in negotiations on the protection of personal data.[2]

1: 2008-12 on the Protection of Personal Data; Articles 5 and following
2: cdp.sn/missions

REGISTRATION

Businesses must notify the CDP in respect of its processing activities, except in the following case:

- Processing for the sole purpose of keeping a register, by law, this is intended exclusively to provide public information and is open to consultation for any person with a legitimate interest.
- The non-profit processing for religious, philosophical, or political associations, or trade unions.[1]

According to Article 22 of the DPA, the declaration must include:

- The identity and address of the Data Controller or his representative;
- Purpose(s) of the processing and the description of its general functions;
- Possible interconnections between databases;
- Personal data processed and categories of persons concerned by the processing;

- Time period for which the data will be kept;
- Department or person(s) in charge of data processing;
- Recipient(s) or categories of recipients of the processed data;
- Persons or departments before which the right of access is exercised;
- Measures taken to ensure the security of the processing; and
- Identity and address of the data processor.

The registration process, following the collection and processing of personal data, must comply with the requirements set by law. Thus, in addition to the prior consent of the author of the information, the registration of data is also subject to the respect of the right to information and the principles of transparency, clarity, confidentiality, compliance with the rules of ethics and ethics governing certain professions.[2]

1: 2008-12 of 25 January 2008 on the Protection of Personal Data, Article 18
2: 2008-12 of 25 January 2008 on the Protection of Personal Data,Article 22

DATA PROTECTION OFFICERS

The law designates a Personal Data Protection Commission (the CDP), whose role it is to ensure that any processing of personal data is in accordance with the law. The commission is also responsible for informing data controllers and data subjects of their rights and obligations, handling complaints, conducting audits, and sanctioning data controllers who are in breach of the law.

COLLECTION & PROCESSING

Processing is any operation performed on personal data. The most common are collection, operation, management, retention or transfer, copying, and to some extent, interconnection.[1]

The controller of personal data is defined as the natural or legal person, public or moral; any other body or association which alone or jointly with others, makes the decision to collect and process personal data and determine the purposes.[2]

The provisions of Article 34 of the aforementioned law requires the person in charge of the procedure to treat personal data lawfully, fairly and not fraudulently. The collection and processing of personal data can not be done freely. The law speaks of a collection for legitimate purposes, for specific explicit purposes.

Personal data must be treated confidentially and be protected, especially if the processing involves data transmissions in a network.[3]

1: 2008-12 of 25 January 2008 on the Protection of Personal Data, Article 4.19
2: 2008-12 of 25 January 2008 on the Protection of Personal Data, Article 4.15
3: 2008-12 of 25 January 2008 on the Protection of Personal Data, Article 38

TRANSFER

Under Senegalese law it is possible to transfer personal data to a third country. When transferring data to a foreign country, the controller is required to submit a duly motivated request to the Personal Data Protection Commission if the transfer lacks an adequate level of protection. This request is possible only when the controller provides a sufficient guarantee of protection of the rights of the data subject regarding compliance with the privacy of the fundamental rights and freedoms of individuals concerned and the exercise of the corresponding rights.

The level of protection in question is assessed in the light of, inter alia, the security measures, the specific processing characteristics such as its purpose, duration, nature, origin and the destination of the processed data.[1]

There are a number of obligations that affect the controller. The data transfer can only be made in a country that offers the same guarantees of protection as Senegal unless the request is accepted.

In derogation of the obligation of the recipient country of the data subject of the transfer, the law provides for the possibility of transferring data to a third country which does not offer the same level of protection, subject to certain conditions.

Indeed, this transfer must be punctual, non-massive and the person to whom the data relates must express his / her consent to a transfer of these data. It must also be expressed if the transfer is necessary to one of the following conditions:

- to safeguard the life of this person;
- the safeguarding of the public interest;
- compliance with obligations to ensure the recognition, exercise or defense of a right to justice;
- to the execution of a contract between the controller and the person concerned, or
- pre-contractual measures taken at the request of the latter.

1: 2008-12 of 25 January 2008 on the protection of personal data, Article 49-51

SECURITY

According to Article 71 of the Protection of Personal Data, all data controllers have an obligation to ensure the security of personal data. The data controller is required to take all necessary precautions with regard to the nature of the data and, in particular, to prevent it from being distorted, damaged, or unauthorized third parties having access to it. Data Controllers must make sure that:

- authorized persons can only access data personal nature within their competence;
- the identity and interests of any third parties recipients of the data can be verified;
- identity of persons having access to the information system can be verified;
- unauthorized persons are prevented from accessing the place and equipment used for data processing;
- unauthorized persons are prevented from reading; coping; modifying, moving and destroying data;
- all data introduced in the system is authorized;
- Data will not be read, copied, modified or erased without authorization during the transport or communication of the data.
- Data is backed up with security copies;
- Data are renewed and converted to preserve them.

BREACH NOTIFICATION

Based on Senegal’s law and regulations there is no legal requirement to report data breaches to the CDP. Nevertheless, the data controller is required to respect confidentiality, security and data retention requirements of the data subject.

There is also no legal requirement for data breaches to be reported to affected individuals.

Mandatory breach notification

No mandatory breach notification protocol is provided under Senegal law.

ENFORCEMENT

The Commission for the Protection of Personal Data has the power to investigate, warn, and sanction. There are three forms of investigations that can be carried out:

- onsite inspections;
- documentary inspections;

- hearing inspections.

The CDP can also send a warning to a controller that does not comply with legal regulations. Six major corporations in 2014 /2015 received warnings and notices from the CDP.

In regards to sanctions, The CDP has the power to carry out civil / administrative sanctions and criminal sanctions. When there is a breach the CDP can carry out a civil or administrative sanction by:

- a provisional withdrawal for three months of the given authorisations; the withdrawal becomes definitive at the end of the three month period if the breach remains.
- fines of between 1 million XOF and 100 Million XOF.
- in urgent cases, the CDP can also interrupt the processing of data for a duration that can not exceed three months.
- lock certain kinds of data for a duration not exceeding three months.
- prohibit processing that does not comply with the regulation.

The CDP can also carry out a criminal sanction consisting of imprisonment between six and seven years; in addition to demanding a fine between 200000 XOF and 10 Million XOF.[1]

1: 2008-12 of 25 January 2008 on the Protection of Personal Data, Articles 29-32

ELECTRONIC MARKETING

According to Article 47, in Senegal it is prohibited for anyone to carry out direct marketing using any means of communication in any form whatsoever, of the data for a staff of a natural person who has not expressed his consent prior to receiving such surveys.[1] It is important to note that Article 47 does not differentiate between the means of marketing but prohibits all direct marketing that lacks prior consent.

Article 16 of the Senegalese Electronic Transactions Law[2] provides more specific regulations on the marketing of data. The following are prohibited:

- direct marketing by sending a message by means of an automated calling machine, a fax machine or an e-mail using, under whatever form the contact details of a natural person who has not expressed its prior consent to receive direct surveys.
- The exception to this, is if the recipient’s details have been collected directly from in accordance with the provisions of the Law on the Protection of Personal data or on the occasion of a sale or supply of services, the direct marketing concerns similar products or services provided by the same natural or legal person, and if the consignee is offered, expressly and unambiguously, the possibility to oppose, without cost, except those related to the transmission of the refusal and in a simple way, to the use of its coordinates when they are collected and whenever an email from propsection is specifically addressed to said person.
- However, in any case, it is prohibited to issue, for direct marketing purposes, messages via automatic calling machines, faxes and emails, without indicating valid details to which the addressee could usefully forward a request to cease the use of their information for marketing.

1: 2008-12 of 25 January 2008 on the Protection of Personal Data, Articles 47
2: Senegalese Electronic Law

ONLINE PRIVACY

The law on Personal Data and the Senegalese Electronic Transactions Law does not contain provisions on online privacy or cookies.

KEY CONTACTS

Geni & Kebe
www.dlapiperafrica.com/senegal

Mouhamed Kebe
Managing Partner
Geni & Kebe
T +221 76 223 63 30
mhkebe@gsklaw.sn

Mahamat Atteib
Associate
Geni & Kebe
T +221 77 737 41 74
m.atteib@gsklaw.sn

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SERBIA

Last modified 17 January 2024

LAW

In late 2018, Serbia updated its data protection law to better align with the EU General Data Protection Regulation. Serbia enacted a new Data Protection Law on 9 November 2018 (published in the Official Gazette of the Republic of Serbia, no. 87 /2018) (“**DP Law**”). Although the DP Law entered into force 21 November 2018, its effective date was postponed until 21 August 2019 (except for the maintenance of the Central Register of Personal Databases which has already been terminated).

The DP Law was long awaited, as it has been 10 years since the previous data protection law was passed. Its content is largely harmonized with the GDPR. It is now fully effective as of 21 August 2019.

DEFINITIONS

Definition of personal data

Under the DP Law, personal data is any information about a natural person through which the respective person is identified or identifiable (for example, name, address, email address, photo, etc.).

NATIONAL DATA PROTECTION AUTHORITY

The Serbian data protection authority is the Commissioner for Information of Public Importance and Protection of Personal Data (*Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti*) (“**DPA**”).

It is seated at Bulevar kralja Aleksandra 15 Belgrade and its website is www.poverenik.rs.

REGISTRATION

The obligation for the maintenance of the Central Register of Personal Databases by the DPA, which existed under the previous data protection law, was terminated immediately upon the entering into force of the DP Law. Under the DP Law, controllers and processors are only required to internally maintain the database records and only if they have more than 250 employees or if they are involved in certain types of processing or process certain types of personal data (such as, for example, special categories of data or personal data relating to criminal convictions and offences). The latter two conditions are applicable regardless of the number of employees a processer or controller has.

DATA PROTECTION OFFICERS

According to the DP Law, controllers and processors are required to designate a data protection officer (“**DPO**”), whose primary task is to ensure compliance with the data processing law and regulations and to communicate with the DPA and the data subjects on all data protection matters. Similar to the GDPR, this obligation applies if the following criteria are met:

- The processing is carried out by a public authority (with the exception of a court performing its judiciary authorizations).
- The core activities of the controller / processor require the regular and systematic monitoring of data subjects on a large scale, or the large-scale processing of special categories of personal data — eg, health data or trade union memberships, or criminal convictions / offences data.

The DPO may be employed or engaged under a service contract, and in any case must have sufficient expert knowledge. A group of companies may appoint a single DPO, provided that he is equally accessible to each company.

Controllers and processors are required to ensure the DPO’s independence in the performance of his tasks. This means the following:

- No instructions may be given to the DPO.
- The DPO must report directly to the manager of the controller / processor.
- The DPO may not be dismissed or penalized for performing his or her tasks.

COLLECTION & PROCESSING

The collection and further processing of personal data has to be legitimate and legally grounded, meaning pursuant to the data subject's consent or as specifically provided by law.

Under the DP Law (substantially the same as under the GDPR), there are a few instances where a data subject's personal data may be processed without the data subject’s consent, as follows:

i. processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
ii. processing is necessary for compliance with a legal obligation to which the data controller is subject;
iii. processing is necessary to protect the vital interests of the data subject or of another natural person;
iv. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; and
v. processing is necessary for the purposes of the legitimate interest pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a minor (i.e. an individual under the age of 18) (“**Specific Cases**”).

Apart from the Specific Cases, prior informed consent from data subjects is generally required to collect and process personal data, meaning that any request for consent has to contain all the information on the particular processing which is explicitly prescribed by the DP Law (for example, the data subject must be notified of the purpose and legal grounds for the processing, information on other recipients of the data in cases when the data is disclosed to entities other than the data controller and information on the statutory rights of the data subjects in relation to the respective processing, etc.).

Although consent is necessary (when none of the Specific Cases is applicable), it does not automatically mean that any processing, to which a data subject has consented will be regarded by the DPA as compliant with the DP Law. There are also other conditions which must be met under the DP Law (e.g. the purpose must be legitimate and clearly determined and the type and scope of processed data must be proportionate to the respective purpose).

In addition to written consent, the DP Law explicitly introduces other forms of consent, such as online consent, oral consent or consent by other clear affirmative action provided that the controller is able to demonstrate that the data subject has indeed consented.

The conditions for obtaining consent have become much stricter under the DP Law than compared to the previous legislation. Similar to the GDPR, consent must be freely given, specific, informed and unambiguous. For example the request for consent — when presented in a written document — must be clearly distinguishable from all other matters, using clear and plain language (meaning catch-all clauses will not be valid). Further, consent will not be considered freely given if the performance of a contract is conditional on the consent to the processing of personal data that is not necessary for its performance.

In addition, one important novelty introduced by the DP Law (and similar to the GDPR), is that it does not apply only to the processing of data carried out by Serbian controllers and processors, but also to the processing of data by controllers and processors based outside of Serbia whose processing activities relate to the offering of goods or services (even if offered for free) or monitoring the behavior of Serbian data subjects within Serbia. As a result, a number of these controllers and processors will need to appoint representatives in Serbia for correspondence with the DPA and the data subjects on all issues related to processing.

TRANSFER

Under the previous data protection law, the DPA’s prior approval was a precondition for a legitimate data transfer whenever a transfer was to be made to any country which had not signed and ratified the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("**Relevant Convention**"). The data transfer regime has now been completely revamped and liberalized under the DP Law, which is a much-welcomed change from the previous overly restrictive concept. The DP Law explicitly applies to both direct and indirect data transfers, unlike the previous law for which it was not fully clear whether it covers indirect transfers at all.

This means that, under the DP Law, substantially the same as under the GDPR, there is a whole set of mechanisms enabling legitimate data transfer out of Serbia. Specifically, subject to circumstances of each particular case, controllers will be entitled to transfer personal data abroad if one of the following situations (among others) occurs:

- Personal data is to be transferred to a country that ratified the Relevant Convention.
- Data transfers are to a country included on the Serbian government’s list of countries providing an adequate level of data protection (EU Countries, other countries which are member states of the Relevant Convention and some other countries such as, for example, Canada (for business subjects only) and Japan).
- Data transfers are performed to a country which has a bilateral agreement with Serbia regulating data transfers.
- The transfer is based on the standard contractual clauses prepared by the Serbian DPA.
- The transfer is based on binding corporate rules or a code of conduct approved by the Serbian DPA, or on certificates issued in accordance with the law.
- The Serbian DPA has issued a specific approval for the transfer to be performed on the basis of an agreement between the data exporter and the data importer.
- The data subject has explicitly consented to the proposed transfer, after having been informed on the possible risks.

This should create more options for the transfer of data to non-European countries, especially since the DPA has prepared the aforementioned standard contractual clauses, which are adopted and applicable as of 30 January 2020 (keeping however in mind that, under the DP Law, the respective SCC mechanism will be available only when a data importer is a data processor). In addition, when it comes to the process of obtaining the DPA’s aforementioned specific approval for a data transfer, such procedure should be completed within 60 days, as explicitly prescribed under the DP Law.

SECURITY

Similar to the GDPR, the DP Law introduces burdensome accountability obligations on data controllers, which are required to "demonstrate compliance”. This includes an obligation to all of the following:

- Implement, maintain and update appropriate technical, organizational and human resources measures to ensure a level of security appropriate to the risk involved by taking into account state of the art and associated implementation costs etc.
- Have in place certain documentation, such as data protection policies and records of processing activities.
  Implement data protection by design and by default.
- Conduct a data protection impact assessments for those processing operations that are likely to cause a high risk to the rights and freedoms of individuals (whereas the specific cases when conducting such assessments is mandatory, are explicitly prescribed as well, e.g. when special categories of personal data are processed on a large scale).

Data protection by design requires the controllers to adopt, as well as maintain and update when needed, appropriate measures (such as pseudonymization, data minimization) which will implement the safeguards necessary for processing. Data protection by default, on the other hand, requires the controllers to adopt measures so that, by default, only the processing which is necessary

for the specific purpose will be possible (e.g. that, by default, privacy settings on one’s social network profile do not make the data public).

BREACH NOTIFICATION

The DP Law imposes data breach notification obligations that largely track the GDPR. Furthermore, the Law on Electronic Communications ('Official Gazette of the Republic of Serbia', no. 35/2023) (“**EC Law**”) imposes a duty on business entities performing electronic communication activities, to notify the Regulatory Body for Electronic Communications and Postal Services (“**RATEL**”) as the competent state authority, of any breach of security and integrity of public communication networks and services, which have influenced their work significantly, whereas RATEL, when it assesses that it is in public interest to publish the respective information, is authorized to inform the public on any such breach or to request from the respective business entity to do that. Additionally, if there is a particular risk of breach of public electronic communication networks and services' security and integrity (e.g. risk of endangering safety of personal data), a business entity is obliged to inform users on such risk and if such risk is out of the scope of the measures the operator is obliged to implement, to inform users on possible measures of protection and costs of their implementation.

Nonperformance of this statutory obligation can lead to liability and fines of up to EUR 17,000 for a legal entity, and up to EUR 1,275 for a responsible person in a legal entity. Protective measures may also be implemented. For a legal entity, a prohibition against performing business activities for a duration of up to three years and for a responsible person in a legal entity, a prohibition against performing certain duties for a duration of up to one year.

According to the DP Law, the data breach obligations present a significant responsibility, as data controllers will generally be required to document each data breach as well as to notify the DPA of such breach (if it may result in a risk to the rights and freedoms of individuals) without undue delay and, when feasible, within 72 hours after becoming aware of the breach. In addition, data processors will have to notify the controllers of the breach without undue delay.

If the personal data breach may result in a high risk to the rights and freedoms of individuals, the controller is also required to communicate the personal data breach to the individual concerned without undue delay. However, this does not apply if the controller has implemented appropriate technical, organizational and human resources measures, such as encryption that has rendered the relevant data unintelligible to any unauthorized person, or has subsequently undertaken measures which ensure that the data breach can no longer lead to consequences for the concerned individual, or, if the notification would involve disproportionate efforts, a public communication or a similar measure must be made in order to properly inform the individuals.

ENFORCEMENT

The DPA is responsible for the enforcement of the DP Law. Namely, the DPA is authorized and obliged to monitor whether the law is implemented and it conducts such monitoring both on its own accord and based on any complaints it receives. If it establishes, when performing the respective monitoring, that a particular person / entity which processes personal data has acted in contravention to the statutory rules on processing, the DPA shall issue a warning to the particular data controller. It may also issue a decision by which it can, among other things:

- Order the data controller to eliminate the existing irregularities within a certain period of time.
- Temporarily forbid particular processing.
- Order deletion of the data collected without a legal ground.

The DPA's decision cannot be appealed, but an administrative dispute can be initiated against the respective decision before a competent Serbian court.

Depending on the gravity of the particular misconduct and the data controller's behavior with respect to the same, the DPA can initiate an offence proceeding against the respective data controller before the competent court. The offences and sanctions for such are explicitly prescribed by the DP Law. The respective sanctions are fines up to EUR 17,000 for a legal entity and up to EUR 1,275 for a responsible person in a legal entity. Additionally, the DPA is now also able to directly fine controllers and processors in certain situations, with fines in the amount of EUR 850. Prior to the adoption of the DP Law, only the Court of Offences was entitled to impose fines.

Criminal liability is also a possibility since the Serbian Criminal Code prescribes a criminal offence of unauthorized collection of personal data. The prescribed sanctions are a fine (of an amount to be determined by the court) or imprisonment of up to one year (i.e. up to three years if the offence is committed by a public official / state servant when performing his duties). Both natural persons and legal entities can be subject to the respective liability.

Formally speaking, under the Law on Administrative Procedure ('Official Gazette of the Republic of Serbia', nos. 18/2016, 95/2018 and 2/2023), the DPA is also authorized to enforce its orders by threatening a company with a fine of up to 10% of its annual income in Serbia in case it fails to comply with the order. This option has not yet been tested in practice, to the best of our knowledge.

ELECTRONIC MARKETING

Electronic marketing is only mentioned in the DP Law in the context of the data subjects' right of complaint. The rules on this subject are envisaged by the Law on Electronic Trade ('Official Gazette of the Republic of Serbia', nos. 41/2009, 95/2013 and 52 /2019), EC Law (as defined above in the section on Breach Notification), the Law on Advertising ('Official Gazette of the Republic of Serbia', nos. 6/2016 and 52/2019) and the Consumer Protection Law (Official Gazette of the Republic of Serbia, no. 88/2021) (together, the **"Relevant Legislation").**

In brief, based on the Relevant Legislation, electronic marketing is only allowed if it is covered by an explicit, prior consent of the person to whom the respective marketing is directed. Additionally, recipients should always be:

- Clearly informed of the identity of the sender and commercial character of the communication (this information should be provided in the Serbian language prior to commencing the marketing).
- Provided with a way to opt out of future marketing messages, at any time and free of charge.

For the sake of completeness, it should be noted that, under the most recent changes from July 2019 of the aforementioned Law on Electronic Trade, the same principle that previous consent is necessary for electronic marketing, i.e. for electronic commercial communication, remained, but it is also envisaged now that certain types of electronic communication shall not be regarded as commercial communication and, consequently, should not be subject to previous consent. Such exempt communications include (1) providing information which enables direct access to business activities of a particular entity such as information on its e-address or e-mail and (2) providing information on a particular entity's goods, services or business reputation if such information is obtained by research or in some other similar way and if it is provided free of charge.

Finally, it is also envisaged by the new Serbian Consumer Protection Law, as referred to above, which became applicable (with the exception of some of its provisions) on 20 December 2021, that it is forbidden to make phone calls and/or send messages by phone to any individuals/consumers whose phone numbers are inscribed in the register of consumers who do not want to receive calls and/or messages as a part of a promotion and/or sales by phone. This register shall be public in its part relating to the phone numbers and date of the inscription in the register. It should also be noted that, regardless of the inscription in this register, consent of a consumer for direct marketing provided to a particular entity/trader before or after the inscription in the register, remains valid until its withdrawal made in line with the DP Law.

ONLINE PRIVACY

There are no specific regulations explicitly governing online privacy (including cookies). Accordingly, the general data protection rules, as introduced by the DP Law are, to the extent applicable, relevant for online privacy as well.

On the other hand, it should be noted that the EC Law, as defined in the section on Breach Notification above, introduces rules on the processing of traffic data and location data, under which business entities performing electronic communication activities are allowed to do the following:

- Process traffic data only as long as such data is necessary for a communication’s transmission and thus, when such necessity ceases to exist, they are obliged to delete the data or to process and keep them in a way that the persons to which the data relates are made unrecognizable, unless in a few explicitly prescribed cases when such obligation does not exist (e.g. if they use the respective data for advertising and services selling purposes on the basis of a data subject's prior consent, to the extent and during the time necessary for the respective purpose).

- Generally process location data only if the persons to which the data relates are made unrecognizable or if they have such persons’ prior consent for the purpose of providing them with value added services in the scope and for the time during which the processing is needed for the respective purpose's realization.

Violations are subject to the fines set forth in Breach notification.

KEY CONTACTS

Karanovic & Nikolic
www.karanovic-nikolic.com/

Sanja Spasenović
Attorney at Law in cooperation with Karanović & Partners
Karanovic & Partners
T +381 11 3094 200/ +381 11 3955 413
sanja.spasenovic@karanovicpartners.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SEYCHELLES

Last modified 17 January 2024

LAW

The Data Protection Act 2023 (the Act) enacted in 2023 replaces the Data Protection Act 2003, which was never brought into force.

The Act itself has not been brought into force yet. Pending the its coming into force, data protection in Seychelles continues to be governed by general principles of privacy and confidentiality in the Civil Code of Seychelles and some provisions of various legislation, eg Financial Institutions Act and Revenue Administration Act.

The principal object of the Act is to provide for the protection of individuals with regards to the processing of personal data and to recognise the right to privacy. The Act seeks to strengthen the control and personal autonomy of data subjects over their personal data in compliance with current relevant international standards and best practice. The Act also seeks to promote and facilitate responsible and transparent flow of information by private and public entities while ensuring respect for individual’s privacy.

DEFINITIONS

Definition of personal data

Personal data is defined under the Act as data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user), including any expression of opinion about the individual but not any indication of the intentions of the data user in respect of that individual.

Definition of sensitive personal data

The Act does not define sensitive personal data. However the Act makes provision for the Minister to modify or supplement the Data Protection Principles set out in the Act for the purpose of providing additional safeguards in relation to personal data consisting of information as to:

- the racial origin of the data subject
- his political opinions or religious or other beliefs
- his physical or mental health or his sexual life, or
- his criminal convictions.

NATIONAL DATA PROTECTION AUTHORITY

The creation of the Office of the Data Protection Commissioner is envisaged by the Act but has not yet taken place.

REGISTRATION

A person shall not hold personal data unless an entry in respect of that person as a data user, or as a data user who also carries on a computer bureau, is for the time being contained in the register of data users maintained by the Data Protection Commissioner.

The particulars to be entered into the data register are as follows:

- the name and address of the data user
- a description of the personal data to be held by it and of the purpose or purposes for which the data is to be held or used
- a description of every source from which it intends or may wish to obtain the data or the information to be contained in the data
- a description of every person to whom it intends or may wish to disclose the data (otherwise than in cases of exemptions from non-disclosure as set out in the Act)
- the name of every country outside Seychelles to which it intends or may wish directly or indirectly to transfer the data, and
- one or more addresses for the receipt of requests from data subjects for access to the data.

A person applying for registration shall state whether he wishes to be registered as a data user, as a person carrying on a computer bureau or as a data user who also carries on a computer bureau, and shall furnish the Data Protection Commissioner with the particulars required to be included in the entry to be made in pursuance of the application. Where a person intends to hold personal data for two or more purposes he may make separate applications for registration in respect of any of those purposes.

A registered person may at any time apply to the Data Protection Commissioner for the alteration of any entries relating to that person. Where the alteration would consist of the addition of a purpose for which personal data are to be held, the person may make a fresh application for registration in respect of the additional purpose.

The Data Protection Commissioner shall, as soon as practicable and in any case within the period of 6 months after receiving an application for registration or for the alteration of registered particulars, notify the applicant in writing whether his application has been accepted or refused. Where the Commissioner notifies an applicant that his application has been accepted, the notification must state the particulars which are to be entered in the register, or the alteration which is to be made, as well as the date on which the particulars were entered or the alteration was made.

No entry shall be retained in the register after the expiration of the initial period of registration except in pursuance of a renewal application made to the Data Protection Commissioner. The initial period of registration and the period for which an entry is to be retained in pursuance of a renewal application ('the renewal period') shall be a period 5 years beginning with the date on which the entry in question was made or, as the case may be, the date on which that entry would fall to be removed if the application had not been made.

The person making an application for registration or a renewal application may in his application specify as the initial period of registration or, as the case may be, as the renewal period, a period shorter than five years, being a period consisting of one or more complete years.

DATA PROTECTION OFFICERS

The Act does not contain any legal requirement to appoint a data protection officer.

COLLECTION & PROCESSING

The data protection principles set out in the Act apply to personal data held by data users. Those data protection principles are as follows:

- the information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully
- personal data shall be held only for one or more specified and lawful purposes
- personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes
- personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes
- personal data shall be accurate and, where necessary, kept up to date
- personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
- an individual shall be entitled:
    - at reasonable intervals, and without undue delay or expenses to be informed by any data user whether he holds personal data of which that individual is the subject
    - to access to any such data held by a data user, and
    - where appropriate, to have such data corrected or erased.

TRANSFER

If it appears to the Data Protection Commissioner that a person registered as a data user (or as a data user who also carries on a computer bureau) intends to transfer personal data held by him to a place outside the Seychelles, the Data Protection Commissioner may, if satisfied that the transfer is likely to contravene or lead to a contravention of any data protection principle, serve that person with a transfer prohibition notice prohibiting him from transferring the data either absolutely or until he has taken such steps as are specified in the notice for protecting the interests of the data subjects in question.

In deciding whether to serve a transfer prohibition notice, the Data Protection Commissioner shall consider whether the notice is required for preventing damage or distress to any person and shall have regard to the general desirability of facilitating the free transfer of data between the Seychelles and other states.

A transfer prohibition notice shall specify the time when it is to take effect and contain a statement of the principle or principles which the Data Protection Commissioner is satisfied are contravened and his reasons for reaching that conclusion, as well as particulars of the right of appeal conferred by the Act.

The Data Protection Commissioner may cancel a transfer prohibition notice by written notification to the person on whom it was served.

No transfer prohibition notice shall prohibit the transfer of any data where the transfer of the information constituting the data is required or authorised by or under any enactment or is required by any convention or other instrument imposing an international obligation on the Seychelles.

Any person who contravenes a transfer prohibition notice shall be guilty of an offence but it shall be a defence for a person charged with an offence under this subsection to prove that he exercised all due diligence to avoid a contravention of the notice in question.

SECURITY

The Act provides that appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

BREACH NOTIFICATION

Breach notification

There is no mandatory requirement in the Act to report data security breaches or losses to the Data Protection Commissioner. However, the Act provides that the Data Protection Commissioner may consider any complaint that any of the data protection principles or any provision of this Act has been or is being contravened and shall do so if the complaint appears to him to raise a matter of substance and to have been made without undue delay by a person directly affected.

Where the Data Protection Commissioner investigates any such complaint he shall notify the complainant of the result of his investigation and of any action which he proposes to take.

Mandatory breach notification

None contained in the Act.

ENFORCEMENT

If the Data Protection Commissioner is satisfied that a registered person has contravened or is contravening any of the data protection principles, the Data Protection Commissioner may serve that person with an enforcement notice requiring him to take such steps for complying with the principle or principles in question. In deciding whether to serve an enforcement notice the Data Protection Commissioner shall consider whether the contravention has caused or is likely to cause any person damage or distress.

An enforcement notice in respect of a contravention of the data protection principle concerning data accuracy may require the user to rectify or erase the data and any other data held by him containing an expression of opinion which appears to the Data Protection Commissioner to be based on the inaccurate data.

If by reason of special circumstances the Data Protection Commissioner considers that the steps required by an enforcement notice should be taken as a matter of urgency, he may include a statement to that effect in the notice.

The Data Protection Commissioner may cancel an enforcement notice by written notification to the person on whom it was served.

Any person who fails to comply with an enforcement notice shall be guilty of an offences; but it shall be a defence for the person charged with an offence under this subsection to prove that he exercised all due diligence to comply with the notice in question.

If the Data Protection Commissioner is satisfied that a registered person has contravened or is contravening any of the data protection principles, the Commissioner may serve the person with a de-registration notice stating that the Data Protection Commissioner proposes to remove from the register all or any of the particulars constituting the entry or any of the entries contained in the register in respect of that person. In deciding whether to serve a de-registration notice, the Data Protection Commissioner shall consider whether the contravention has caused or is likely to cause any person damage or distress, and the Data Protection Commissioner shall not serve such a notice unless he is satisfied that compliance with the principle or principles in question cannot be adequately secured by the service of an enforcement notice.

ELECTRONIC MARKETING

Although not specifically provided for in the Act, the latter will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (for instance, an email is likely to be considered as personal data for the purposes of the Act).

ONLINE PRIVACY

The Act does not contain specific provisions in relation to online privacy.

KEY CONTACTS

Juristconsult Chambers
www.juristconsult.com

Shalinee Dreepaul Halkhoree
Partner-Barrister
Juristconsult Chambers
T +230 465 00 20 Extension 225
sdreepaul@juristconsult.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SINGAPORE

Last modified 20 December 2023

LAW

Singapore enacted the Personal Data Protection Act of 2012 (No. 26 of 2012) on October 15, 2012, and it was subsequently amended / enhanced via the Personal Data Protection (Amendment) Act 2020 (together, the “**Act**”).

The Act has extraterritorial effect, meaning it applies to organizations collecting, using or disclosing personal data in Singapore whether or not the organization itself has a physical presence or is registered as a company in Singapore.

In addition to the Act, the Singapore data protection regime consists of various general or sector / industry-specific guidelines issued by the Personal Data Protection Commission (“**Commission**”). While these guidelines are advisory in nature and not legally binding, they indicate the manner in which the Commission will interpret the Act. Therefore, it is best practice to carefully observe and follow these guidelines.

The data protection obligations under the Act do not apply to the public sector, to whom separate rules under the Government Instruction Manual 8 (“**IM8**”) and the Public Sector (Governance) Act apply. Collectively, these rules provide comparable standards of data protection compared to the Act, including similar investigations and enforcement actions taken against data security breaches. The Public Sector Data Security Review Committee was convened on March 31, 2019 to conduct a comprehensive review of data security policies and practices across the public sector. The Government implemented its recommendations and adopted changes to its data security measures. Examples include:

- Requiring officers to password-protect files containing sensitive data when sending out; and
- Enhancing the data incident management framework with standardized process to notify affected individuals in data incidents and conduct post-incident inquiry.

DEFINITIONS

Definition of personal data

Personal data is defined in the Act to mean data, whether true or not, about an individual (whether living or recently deceased*) who can be identified from:

- that data; or
- that data and other information to which the organization has, or is likely to have access.

*The Act's application to recently deceased individuals is limited to disclosure and protection of personal data where such data is about an individual who has been deceased for ten years or fewer.

The data protection obligations under the Act do not apply to business contact information. This excludes from the Act the following if provided solely for business purposes:

- Name
- Position name or title
- Business telephone number
- Business address
- Business electronic mail address
- Business fax number

It is important to note that the Act still governs business contact information provided by individuals solely in their personal capacity. Where the purposes of provision of business contact information are mixed (that is, for both business and personal purposes), the Act does not apply.

Definition of sensitive personal data

There is no definition of sensitive personal data in the Act.

However, non-binding guidance from the Commission indicates that sensitivity of data is a factor for consideration in implementing policies and procedures to ensure appropriate levels of security for personal data. For example, encryption is recommended for sensitive data stored in an electronic medium that has a higher risk of adversely affecting the individual should it be compromised. Where any personal data collected is particularly sensitive (e.g. regarding physical or mental health), as a matter of best practice, such data should only be used for limited purposes and the security measures afforded to such data should take into account the sensitivity of the data.

In addition, the non-binding guidelines issued by the Commission also provide that, in its calculation of financial penalties for breaches of the Act, the Commission would consider whether the organization in question is in the business of handling large volumes of sensitive personal data, the disclosure of which may cause exceptional damage, injury or hardship to an individual (such as medical or financial data), but it has failed to put in place adequate safeguards proportional to the harm that might be caused by disclosure of such personal data.

The Commission has also issued a set of advisory guidelines to impose restrictions on the collection, use and disclosure of National Identification Registration Card (“**NRIC**”) numbers, due to the sensitive nature of the information contained in NRICs (and other similar forms of identification). Organizations are not permitted to collect either the NRIC number or the physical cards or other similar forms of identification unless the organization is permitted to do so under the law or if the collection is necessary for the verification of an individual's identity to “high degree of fidelity” (where it is extremely important the individual’s identity is verified, and failure to do so may, for example, pose a significant safety or security risk).

NATIONAL DATA PROTECTION AUTHORITY

Personal Data Protection Commission

Address

10 Pasir Panjang Road #03-01
Mapletree Business City
Singapore 117438

Telephone

+65 6377 3131

Fax

+65 6577 3888

Email

info@pdpc.gov.sg

Website

www.pdpc.gov.sg

REGISTRATION

There are no registration requirements under the Act.

While not a requirement, the Commission strongly encourages organizations to register their Data Protection Officers ("**DPOs**") with the Commission via the Commission's website, to assist DPOs in keeping up to date with developments in the law. Organisations may also choose to register their DPOs’ business contact information as part of their Accounting and Corporate Regulatory Authority (“**ACRA**”) Bizfile details, so that these will show up in search results on the ACRA website.

DATA PROTECTION OFFICERS

It is mandatory for each organization to appoint one or more DPOs to be responsible for ensuring the organization’s compliance with the Act. An organization may appoint one person or a team of persons to be its DPO. Once appointed, the DPO may in turn delegate certain responsibilities, including to non-employees of the organization. The business contact information of the DPO must be made available to the public.

While there is no requirement for the DPO to be a citizen or resident in Singapore, the Commission suggests that the DPO should be readily contactable from Singapore, available during Singapore business hours and, where telephone numbers are provided, these should be Singapore telephone numbers.

Failure to appoint a DPO may lead to a preliminary investigation by the Commission. If an organization or an individual fails to cooperate with the investigation, this will constitute an offence. As a result, an individual may be subject to a fine of up to SGD 10,000 or imprisonment for a term not exceeding 12 months, or to both. An organization may be subject to a fine of up to SGD 100,000.

COLLECTION & PROCESSING

Organizations may only collect, use or disclose personal data in the following scenarios:

- They obtain express consent from the individual prior to the collection, use, or disclosure of the personal data (and such consent must not be a condition of providing a product or service, beyond what is reasonable to provide such product or service; and must not be obtained through the provision of false or misleading information or through deceptive or misleading practices), and have also provided the relevant data protection notice (notifying purposes of collection, use and disclosure) to the individual before, or at the time when they are collecting, using or disclosing the personal data. It is also possible to obtain the deemed consent of the individual to the collection, use, or disclosure of the personal data in accordance with the relevant conditions of the Act (see the Personal Data Protection Regulations 2021).
- Where the limited specific exclusions prescribed in the Act apply (if no consent or deemed consent is given). Such exclusions include vital interests of individuals, matters affecting public, legitimate interests, business asset transactions, business improvement purposes and other additional bases.

The Act currently in force expanded the concept of “deemed consent” to cover circumstances where: (i) the collection, use or disclosure of personal data is reasonably necessary to conclude or perform a contract or transaction; or (ii) (a) where individuals have been notified of the purpose of the intended collection, use or disclosure of personal data, given a reasonable opportunity to opt-out, and have not opted out, and (b) the organization has conducted an assessment on the likely

adverse effect on such individuals, and identified and put in place reasonable measures to eliminate, reduce the likelihood of or mitigate any such adverse effect.

An individual may at any time withdraw any consent given, or deemed given under the Act, upon giving reasonable notice to the organization.

Further, any collection, use or disclosure of the personal data must only be for the purposes that a reasonable person would consider appropriate in the circumstances, and for purposes to which the individual has been notified of. Such notification must be made in accordance with the requirements of the Act.

An organization must also do all of the following:

- Make information about its data protection policies, practices and complaints process publicly available.
- Cease to retain personal data or anonymize it where it is no longer necessary for any business or legal purpose. Ensure personal data collected is accurate and complete if likely to be used to make a decision about the individual or disclosed.
- Respond to requests by data subjects under their statutory rights, including a new right of data portability (this right is expected to come into force soon).

Data intermediaries that process personal data on behalf of another organization (i.e. data controller) pursuant to a written contract are exempt from most of the data protection obligations under the PDPA. However, data intermediaries are directly liable under two specific obligations relating to the retention (see above) and protection (see Security) of personal data.

Data protection management program (“**DPMP**”) and data protection impact assessment (“**DPIA**”) guides were published by the Commission in November 2017 and updated in September 2021.

TRANSFER

In disclosing or transferring personal data to onshore third parties (including affiliates), an organization should ensure that it has obtained the individual's deemed or express consent to such transfer (unless exemptions apply) and, if this was not done at the time the data was collected, additional consent will be required (unless exemptions apply).

It is also a requirement under the Act for organizations to enter into written agreements with their data intermediaries to whom they transfer personal data and who process such data on behalf of the organizations.

The Act also contains offshore transfer restrictions, which require an organization to ensure that the receiving organization has in place "comparable protection" to the standards set out in the Act when transferring personal data outside of Singapore. Mechanisms to achieve this include (this is not a comprehensive list): data transfer agreements (for which the Commission has released suggested sample clauses); the individual has given consent (provided required notices have been given to the individual setting out the basis upon which their data will be protected in the country or territory to which their personal data will be transferred); and where transfers are considered necessary in certain prescribed circumstances (which include in connection with performance of contracts between the transferring organization and the individual, subject to certain conditions being met). An organization may apply to be exempted from any requirement prescribed under the Act in respect of any transfer of personal data out of Singapore. An exemption may be granted on such conditions as the Commission may require.

The Amendment Act provides for a new right of data portability on electronic data (this right is expected to come into force soon). Individuals may request an organization (“**Porting Organization**”) to transmit certain data about them to another organization. The Porting Organization must have an ongoing relationship with the individual, and have collected or created such data.

The Commission has published guides to data sharing (covering intragroup and third party sharing) with practical nonbinding guidance on data transfer / sharing for organizations, as well as DPMP and DPIA guides (see Collection & Processing).

SECURITY

Organizations must protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, the loss of any storage medium or

device on which personal data is stored, or similar risks. Data intermediaries are also directly liable and subject to the same security obligation. The Act does not specify security measures to adopt and implement, however the Commission has issued best practice guidance which provides specific examples, including with respect to cloud computing and IT outsourcing.

BREACH NOTIFICATION

Under the current Act, where an organization has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, it must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a “notifiable data breach” (as defined in the current Act). A data breach means (a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data, or (b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur. A data breach constitutes a “notifiable data breach” if:

i. it results in, or is likely to result in, significant harm to the affected individuals (including one that compromises personal data prescribed under the Personal Data Protection (Notification of Data Breaches) Regulations 2021); or
ii. it is of a significant scale (i.e. one that affects 500 or more individuals).

An organization must notify the Commission as soon as practicable and in any case no later than three calendar days after the day the organization makes the above assessment of a notifiable data breach. If the data breach results in, or is likely to result in, significant harm to the affected individual(s), an organization must also notify each affected individual in any manner that is reasonable in the circumstances.

The Personal Data Protection (Notification of Data Breaches) 2021 sets out the list of information to be included in notifications to the Commission and affected individuals.

Where a data breach is discovered by a data intermediary, the data intermediary must notify the organization (i.e. data controller) without undue delay from the time the data intermediary has credible grounds to believe that a data breach has occurred in relation to personal data that it is processing on behalf of and for the purposes of the organization. Upon notification by the data intermediary, the organization must conduct an assessment of whether the data breach is a notifiable data breach.

In addition, the Cybersecurity Act 2018 (“**CSA**”) was passed in Singapore in early 2019. The CSA primarily contains obligations applicable to organizations which have been designated as owners of critical information infrastructure. In particular, if your organization has been designated by the Cybersecurity Commissioner as the owner of a critical information infrastructure, additional obligations will apply to your organization in relation to data breach incident handling and notification. Amendments were proposed to the CSA in December 2023, with the Cybersecurity (Amendment) Bill (Bill) made available for public consultation until early January 2024. The Bill proposes imposing obligations on other operators of digital infrastructure and technology, to ensure that the CSA keeps pace with technological developments and industry practices.

ENFORCEMENT

Enforcement of the Act is carried out by the Commission, which include giving directions to an organization to do any of the following:

- Stop collection, use or disclosure of personal data in contravention of the Act;
- Destroy personal data collected in contravention of the Act;
- Provide or refuse access to or correction of personal data;
- Pay a financial penalty of either up to (i) 10% of an organization’s annual turnover in Singapore for those with annual turnover in Singapore that exceeds SGD 10 million, or (ii) SGD 1 million.

These directions may be registered with the Singapore District Courts so that they may have the force and effect of an order of court.

The Commission issued revised Advisory Guidelines on Enforcement Data Protection Provisions on 1 February 2021.

Further, new criminal offences are in force to hold individuals accountable for egregious mishandling of personal data, including knowing or reckless unauthorized disclosure, unauthorised re-identification of anonymized data, or use of personal data for a gain or to cause harm or loss to another person.

Guidelines published by the Commission indicate how in practice the Commission proposes to handle complaints, reviews and investigations of breaches of the data protection rules under the Act, and to approach enforcement and sanctions. Amongst other things, they set out the Commission's enforcement objectives, and guidance regarding the mitigating and aggravating factors that the Commission will take into account when issuing directions and sanctions (for example, prompt initial response and resolution of incidents; cooperation with investigations; and breach notification). The Commission has in the past couple of years stepped up its efforts to enforce the Act, highlighting the growing risks of non-compliance with the Act in Singapore.

Directions or decisions given are subject to reconsideration by the Commission, upon written application by any aggrieved party.

Directions, decisions or reconsiderations of the Commission may also be subject to appeal to a Data Protection Appeal Committee, unless the direction or decision to be appealed is the subject of an application for reconsideration, in which case such appeal would be deemed withdrawn.

Directions may only be appealed to the High Court and Court of Appeal with regard to the following:

- A point of law arising from a direction or decision of the Appeal Committee
- Any direction of the Appeal Committee as to the amount of a financial penalty

Any person who has suffered loss or damage directly as a result of a contravention of the Act is also entitled to pursue a private action in court. However, where the Commission has made a decision with regard to the said loss or damage, a right of private action will only be possible after the decision has become final as a result of there being no further right of appeal. The court may grant to the plaintiff all or any of the following:

- Relief by way of injunction or declaration
- Damages
- Such other relief as the court thinks fit

ELECTRONIC MARKETING

The data protection principles in the Act apply to any marketing activities (including electronic marketing) which involve the collection, use or disclosure of personal data.

In addition, any organization or person that wishes to engage in any telemarketing activities will need to comply with the "Do Not Call" provisions under the Act. Generally, a person or organization who wishes to send marketing messages to a Singapore telephone number should first obtain the clear and unambiguous consent of the individual to the sending of the messages to such Singapore telephone number. The consent must:

- be evidenced in written or other form so as to be accessible for subsequent reference;
- not be a condition for supplying goods, services, land, interest or opportunity; and
- not be obtained through the provision of false or misleading information or through deceptive or misleading practices.

In the absence of such consent, organizations must check and ensure that the telephone number is not on a Do-Not-Call register maintained by the Commission (“DNC Register”). There are also other requirements, including a duty to identify the sender of the marketing message and provide clear and accurate contact information, as well as a duty not to conceal the calling line identity of any voice calls containing such marketing messages. An individual may at any time apply to the Commission to add or remove his Singapore telephone number on the DNC Register.

Further, the current Act provides the role of “checkers” which are entities that provide information for gain on whether a Singapore telephone number is listed in the DNC Register for the purposes of another organization’s obligations under the Act. It imposes obligations on third party checkers, and checkers will be liable for DNC infringements resulting from any erroneous information provided by them.

The Act will apply to marketing messages addressed to a Singapore telephone number in the following circumstances:

- The sender of the marketing message is present in Singapore when the message was sent.
- The recipient of the marketing message is present in Singapore when the message is accessed.

Electronic marketing activities are also regulated under the Spam Control Act 2007 (**"SCA"**), to the extent that such activities involve the sending of unsolicited commercial communications in bulk by electronic mail or by SMS or MMS to a mobile telephone number.

The DNC provisions under the current Act include a prohibition on sending messages to telephone numbers generated or obtained through dictionary attacks (generating telephone numbers by combining numbers into numerous permutations) or address-harvesting software. Related amendments to the SCA to prohibit sending unsolicited electronic messages to instant messaging accounts are also in force.

The Commission issued the revised Advisory Guidelines on the Do Not Call Provisions on February 1, 2021.

ONLINE PRIVACY

Currently, there are no specific requirements relating to online privacy (including cookies and location) under the Act. Nevertheless, an organization that wishes to engage in any online activity that involves the collection, use or disclosure of personal data will still need to comply with the general data protection obligations under the Act. For example, if an organization intends to use cookies to collect personal data, it must obtain consent before use of any such cookies. For details of the consent required, please see Collection & Processing. The Commission has published nonbinding guidelines providing practical tips on pertinent topics such as securing electronic personal data, building websites, the capture of IP addresses and the use of cookies.

KEY CONTACTS

Carolyn Bigg
Partner, Global Co-Chair of Data Protection, Privacy and Security Group
T +852 2103 0576
carolyn.bigg@dlapiper.com

Yue Lin Lee
Senior Associate
T +852 2103 0890
yuelin.lee@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SINT MAARTEN

Last modified 28 January 2024

LAW

- **National ordinance personal data protection** *(Landsverordening bescherming persoonsgegevens*, National Gazette 2010, Consolidated text no. 2) “(National Ordinance Personal Data Protection”);
- **General Data Protection Regulation** (the “GDPR”) – a regulation of the European Union which became effective on May 25, 2018 – may have implications for a data controller / data processor as the extra-territorial reach of the GDPR is not only relevant to businesses established in the European Union but also to international businesses established in Sint Maarten which offer goods or services to individuals in the European Union or monitor their behaviour in the European Union.

DEFINITIONS

Definition of Personal Data

National Ordinance Personal Data Protection

According to the Explanatory Memorandum on the National Ordinance Personal Data Protection the term personal data has a broad meaning. This does not only concern data that can identify a person, but concerns any data that can be associated with a particular person; it is foreseeable that under certain circumstances data can be traced to one person through systematic comparison and lengthy investigations. Personal identifiable confidential data is therefore not only limited to home address, email address, telephone number, membership number and/or identity number.

GDPR

Personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Definition of Sensitive Personal Data

National Ordinance Personal Data Protection

A person’s religion or belief, race, political views, health, sexual life as well as personal data concerning membership of a trade union.

GDPR

Data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

NATIONAL DATA PROTECTION AUTHORITY

National Ordinance Personal Data Protection

The Personal Data Protection Committee as referred to in article 42 of the National Ordinance Personal Data Protection.

GDPR

An independent public authority established by a Member state pursuant to article 51 of the GDPR (Article 4(21), GDPR). The authority is responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the EU.

REGISTRATION

National Ordinance Personal Data Protection

No registration required.

GDPR

Article 30 GDPR requires companies to keep an internal electronic registry, which contains the information of all personal data processing activities carried out by the company.

DATA PROTECTION OFFICERS

National Ordinance Personal Data Protection

Pursuant to article 13 of the National Ordinance Personal Data Protection the responsible party shall execute appropriate technical and organizational measures to secure personal data against loss or any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking account of the technical state of the art and the costs of execution, in view of the risks associated with that processing and the nature of the data to be protected. The measures shall be aimed partly at preventing unnecessary gathering and further processing of personal data.

Besides the measures above, the National Ordinance Personal Data Protection does not contain any clauses on any type of registration, filings of documents to any public agency or having a mandatory data protection officer in place.

GDPR

The appointment of a data protection officer under the GDPR is only mandatory in three situations:

- When the organisation is a public authority or body;
- If the core activities require regular and systematic monitoring of data subjects on a large scale; or
- If the core activities involve large scale processing of special categories of personal data and data relating to criminal convictions.

COLLECTION & PROCESSING

National Ordinance Personal Data Protection

Collection: a natural or legal person, public authority, agency or other body which who has control over a person registration.

Processor: a natural or legal person, public authority, agency or other body which who owns all or part of the has equipment in his possession, with which a personal registration of which he is not the holder.

GDPR

Collection: a natural or legal person, public authority, agency or other body that collect personal data and use it for certain purposes, like a website that markets to users based on their online behaviour.

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority.

TRANSFER

National Ordinance Personal Data Protection

Contains no clauses.

GDPR

The GDPR restricts transfers of personal data outside the European Economic Area, or the protection of the GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.

SECURITY

National Ordinance Personal Data Protection

Pursuant to article 13 of the National Ordinance Personal Data Protection the responsible party shall execute appropriate technical and organizational measures to secure personal data against loss or any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking account of the technical state of the art and the costs of execution, in view of the risks associated with that processing and the nature of the data to be protected. The measures shall be aimed partly at preventing unnecessary gathering and further processing of personal data.

GDPR

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (article 32 GDPR).

BREACH NOTIFICATION

National Ordinance Personal Data Protection

Contains no specific clauses.

GDPR

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with article 55 GDPR, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

ENFORCEMENT

National Ordinance Personal Data Protection

Pursuant to article 60 the responsible party who acts in contravention of the provisions of the National Ordinance Personal Data Protection may be penalized by the Sint Maarten committee of data protection with a financial penalty in the minimum amount of Naf. 1,000 (USD 571.43) maximum amount of Naf. 500,000.00 (USD. 277,777.78).

GDPR

The GDPR holds a variety of potential penalties for businesses.

For example, article 77 of GDPR states that:

“Every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating him or her infringes this Regulation.”

Additionally, article 79 of the Regulation states that *“such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence.”*

Penalties

Compensation to Data Subjects. One penalty that may be imposed is compensation to, as stated in article 82 of the Regulation, *“Any person who has suffered material or non-material damage as a result of an infringement of this Regulation”* for the damage they’ve suffered.

Fines

Article 83 of GDPR specifies a number of different fines that may vary based on the nature of the infraction, its severity, and the level of cooperation that “data processors” (i.e. you) provide to the “supervisory authority.” Less severe infringements may incur administrative fines of up to 10,000,000 Euros or 2% of your total worldwide annual turnover for the preceding year (whichever is greater), while more severe infractions may double these fines (20,000,000 or 4% annual turnover).

Individual Member States of the EU may have additional fines and penalties that may be applied as well. However, these additional penalties are not specifically listed in the text of the Regulation since they’re up to the individual EU nations to set— the only guidelines in article 84 of GDPR are that *“Such penalties shall be effective, proportionate and dissuasive”* and that *“Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018.”*

ELECTRONIC MARKETING

National Ordinance Personal Data Protection

N/A.

GDPR

Under article 22 GDPR organizations cannot send marketing emails without active, specific consent.

Companies can only send email marketing to individuals if:

- The individual has specifically consented.
- They are an existing customer who previously bought a similar service or product and were given a simple way to opt out.

ONLINE PRIVACY

National Ordinance Personal Data Protection

Contains no specific clauses.

GDPR

Cookies, insofar as they are used to identify users, qualify as personal data and are therefore subject to the GDPR. Companies do have a right to process their users’ data as long as they receive consent or if they have a legitimate interest.

Location data, the GDPR will apply if the data collector collects the location data from the device and if it can be used to identify a person.

If the data is anonymized such that it cannot be linked to a person, then the GDPR will not apply. However, if the location data is processed with other data related to a user, the device or the user’s behavior, or is used in a manner to single out individuals from others, then it will be “personal data” and fall within the scope of the GDPR even if traditional identifiers such as name, address etc. are not known.

KEY CONTACTS

HBN Law & Tax
hbnlawtax.com/

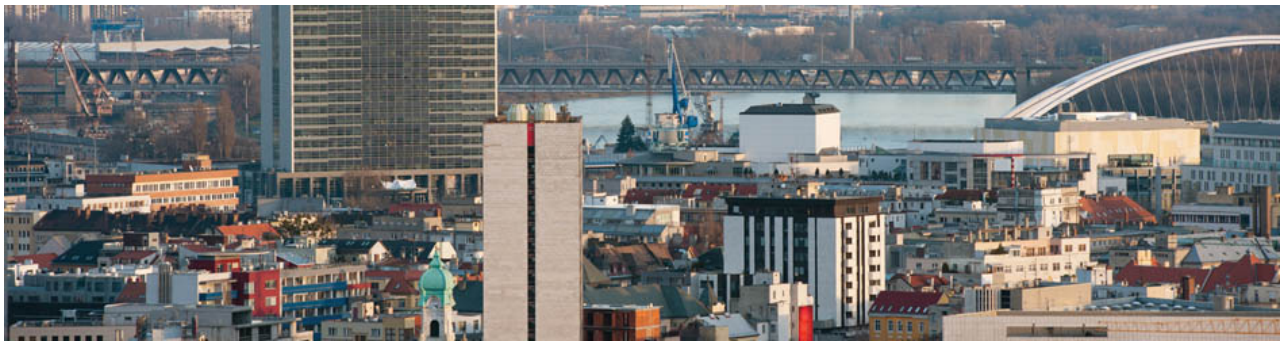
Maarten Willems
Senior Associate
HBN Law & Tax
T +297 588 6060
maarten.willems@hbnlawtax.com

Misha Bemer
Partner
HBN Law & Tax
T +297 588 6060
misha.bemer@hbnlawtax.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SLOVAK REPUBLIC



Last modified 17 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

As a member of the European Union, Slovakia is bound by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (the "**GDPR** ").

Furthermore, Slovakia adopted Act No. 18/2018 Coll. on the protection of personal data and on amending and supplementing certain acts (the "**Slovak Data Protection Act**") implementing the GDPR, which became effective as of 25 May 2018.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for " *identifiable*" – if the natural person can be identified using “all means reasonably likely to be used” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions provided by the GDPR apply.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (similar to the CNIL in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the GDPR.

The GDPR creates the concept of "**lead supervisory authority**." Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by, and answer to, the supervisory authority for their main or single establishment, the so-called "lead supervisory authority."

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory. The concept of lead supervisory authority is therefore of somewhat limited use to multinationals.

The Data Protection Office of the Slovak Republic (the ‘Slovak Office’) is:

Úrad na ochranu osobných údajov Slovenskej republiky (Official Slovak Name)

Hraničná 12
820 07, *Bratislava* 27
Slovak Republic

The Slovak Office is the supervisory authority and is responsible for overseeing the Slovak Data Protection Act and the GDPR in Slovakia.

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

There is no registration or notice obligation to the Slovak Office as supervisory authority required anymore.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

There is an online form on the website of the Slovak Office which should be completed in order to notify the supervisory authority of the appointment of a DPO.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be:

- Processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle")
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle")
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- Accurate and where necessary kept up to date (the "accuracy principle")
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle")
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle")

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance for potentially years after a particular decision relating to processing personal data was rendered. Record-keeping, auditing and appropriate governance will all play a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies

- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices
- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law. (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to re-purpose personal data - ie, use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymisation

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing

- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

The Court of Justice of the European Union delivered two judgments on 24 September 2019 in case of 'Right to be forgotten'.

The first decision of the CJEU provides important explanations on the conditions under which persons may delete a link found in a search result if the linked page contains information related to sensitive information (such as their religion, their political opinion or the existence of a conviction for crime). It also provides useful information about the public's interest in accessing information that has become incomplete or outdated due to the passage of time (Judgment of the CJEU in Case C-136/17).

In its second decision, the CJEU decided on the geographical scope of the right to remove links from search results after entering the first name and last name. The CJEU limits the effect of the right of removal from search results to results from European territory only - in other words, removing results in the EU but not worldwide. Search results will therefore remain accessible based on searches conducted outside the European Union. (Judgment of the CJEU in Case C-507/17).

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (eg, commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

1. Necessary for entering into or performing a contract
2. Authorised by EU or Member State law
3. The data subject has given their explicit (ie, opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Collection and processing of personal data is governed by the GDPR.

However, there is specific regulation in this respect in the fourth part of the Slovak Data Protection Act. Pursuant to Section 78 of the Slovak Data Protection Act, these specific situations are as follows:

- A controller may process personal data without the consent of a data subject if the processing of personal data is necessary for academic, artistic or for literary purposes;
- A controller may process personal data without the consent of a data subject if the processing of personal data is necessary for the purposes of informing the public by means of mass media and if the personal data are processed by a controller which is authorised to do such business activity;
- A controller who is the employer of a data subject is authorized to provide his / her personal data or to make public his / her personal data in the scope of academic title, name, surname, position, personal employee´s number, department, place of work performance, telephone number, fax number, work email address and the identification details of employer, if this is necessary in connection with the performance of the employment duties of a data subject. Such provision of personal data or making them public shall not interfere with the reputability, dignity and security of a data subject;
- In the processing of personal data, a birth number may be used for the purpose of identifying a natural person only if its use is necessary for the purpose of processing. A data subject shall grant the explicit consent. Processing of a birth number on the legal basis of consent of a data subject shall not be excluded by a special regulation. Making public a birth number is prohibited; this does not apply if a data subject makes public a birth number;

- A controller may process genetic, biometric and health-related data on the legal basis of a special regulation or an international treaty to which the Slovak Republic is bound;
- Personal data on the data subject may be obtained from another natural person and processed in the information system with the prior written consent of data subject only; this does not apply if another natural person by providing personal data about the data subject to the information system, protects his own rights or legally protected interests, reports the facts that justify the application of legal liability of the data subject or personal data are processed on the basis of a special act. Upon request of Office, the person who processes such personal data must be able to prove to the Office that he / she has obtained personal data in accordance with this act.
- If a data subject is dead, the consent required may be given by a close person. The consent is not valid if at least one close person has disagreed in writing.
- If a data subject is dead, the consent required may be given by a close person. The consent is not valid if at least one close person has disagreed in writing.
- When processing personal data for archiving, scientific purposes, historical research or statistical purposes, the controller and the intermediary are obliged to accept adequate guarantees for the rights of the data subject. These guarantees shall include the establishment of adequate and effective technical and organizational measures, in particular to ensure compliance with the principles of data minimization and pseudonymisation. This does not apply to the processing of personal data of deceased persons.

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, Eastern Republic of Uruguay, New Zealand and the United Kingdom.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules and standard contractual clauses. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR (Article 49) also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in

force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

Pursuant to the GDPR, the free movement of personal data between the Slovak Republic and EU Member States is guaranteed; the Slovak Republic shall not restrict or prohibit the transfer of personal data in order to protect the fundamental rights of natural persons, in particular their right to privacy in connection with the processing of their personal data.

The transfer of personal data to third countries or international organisations is governed by the GDPR.

SECURITY

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The rights and obligations in regard to the security of personal data are governed by the GDPR.

In this respect, the Slovak Office issued Decree No. 158/2018 Coll. on Procedure when Assessing the Impact on the Protection of Personal Data as of 29 May 2018.

Controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The rights and obligations in regard to the security of personal data are governed by the GDPR.

In this respect, the Slovak Office issued Decree No. 158/2018 Coll. on Procedure when Assessing the Impact on the Protection of Personal Data as of 29 May 2018.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*." (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and

freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay. (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach. (Article 33(2)).

The notification to the supervisory authority must include where possible:

- The categories and approximate numbers of individuals and records concerned
- The name of the organisation’s data protection officer or other contact
- The likely consequences of the breach and the measures taken to mitigate harm
- The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Controllers are also required to keep a record of all data breaches (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

Breach notifications are governed by the GDPR.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;

- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The Slovak Office has various powers to ensure compliance with the Slovak Data Protection Act and the GDPR.

For example, the Slovak Office is entitled to:

- on request, provide information to a data subject in relation to the exercise of her / his rights;
- order a controller or a processor to provide the necessary information;
- order a data controller to notify a data subject of a personal data breach;
- enter the premises of a controller or a processor;
- impose a corrective measure or a fine.

ELECTRONIC MARKETING

With effect as of 1 February 2022, the electronic marketing is regulated by the Act No. 452/2021 Coll. on Electronic Communications, as amended (the “**Act**”). With the effectiveness of the Act, the former regulation, i.e. Act No. 351/2011 Coll. on Electronic Communications, as amended, has been repealed.

The Act transposed Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing a European Electronic Communications Code into the Slovak law.

The Act introduced new requirements for obtaining consent and conditions for conducting direct marketing including its definition.

According to the Act, the direct marketing means any form of presentation of goods or services in written or oral form, sent or presented through a publicly available service directly to one or more subscribers or users.

The Act stipulates that the use of automatic call and communication systems without human intervention, fax, e-mail and SMS and MMS message service is permitted towards the subscriber or user only with his / her prior demonstrable consent obtained before contacting the subscriber or user. For the purposes of obtaining prior consent, the use of automatic calling and communication systems without human intervention, fax, electronic mail and short message service is prohibited.

Consent that meets the requirements of Article 4 (11) GDPR is considered to be demonstrable consent for the purposes of direct marketing. The person to whom such consent was granted is obliged to keep a durable medium on which the demonstrable consent of the subscriber or user is recorded for a period of at least four years from the withdrawal of the consent by the subscriber or user. When obtaining the consent of the subscriber or user, the person carrying out direct marketing is obliged to indicate the way in which the consent can be easily revoked.

The subscriber or user can at any time withdraw the previous consent or object to the call for the purpose of direct marketing or obtaining consent. The person to whom such consent has been revoked or to whom the call has been objected is obliged to demonstrably confirm to the subscriber or user the revocation of such consent or the acceptance of the objection to the call no later than 30 days after the date of revocation of consent or the receipt of the objection to the call and to keep the confirmation of the revocation of the consent or the acceptance of the objection to the call on a durable medium for a period of at least four years from the withdrawal of consent or call objections.

The Act introduced also the list of the phone numbers, which will be held by the Office for Electronic Communications and Postal Services and which will include the phone numbers stipulated by subscribers or users for the purpose of expressing disagreement with the call for direct marketing purposes and for verifying the listing of a telephone number or group of telephone numbers by the person carrying out direct marketing in the list of telephone numbers (the “**list**”).

For the purposes of direct marketing, any call is prohibited if the subscriber or user has:

- provided a phone number in the list; or
- objected to such calls to the person for whose benefit direct marketing is carried out (this does not apply if the subscriber or user revoked the objection to calls for the purposes of direct marketing to the person for whose benefit direct marketing is carried out or granted his / her consent in the time after the last update of the phone number in the list).

The prior consent of the recipient of electronic mail, SMS and MMS message service is not required if it is a direct marketing of a person's own similar goods and services, and if his / her contact details for the delivery of electronic mail, SMS and MMS message service were obtained by the same person in connection with the sale of goods or services, or if it is direct marketing addressed to the published contact details of subscriber or user who is a natural person - entrepreneur or legal entity. The recipient of electronic mail, SMS and MMS message service must be given the opportunity to simply and free of charge at any time to refuse such use of the contact data at the time of their acquisition and with each delivered message if he / she has not previously refused such use. It is forbidden:

i. to send electronic mail from which the identity and address of the sender is unknown, to which the recipient can send a request to stop sending such messages; and
ii. to encourage visitors to visit a website in violation with a special regulation.

ONLINE PRIVACY

As regards the protection of privacy and protection of personal data processed in the electronic communications sector, the provisions of the Act (Act No. 452/2021 Coll. On Electronic Communications, as amended) shall apply. The Act implemented e.g. Directive 2002/58/EC (as amended by Directive 2009/136/EC).

Under the Act, the undertaking company that provides a publicly available network or service or a provider of a publicly available service is obliged to ensure the technical and organizational confidentiality of messages and associated Traffic Data that are

transmitted through its public network and publicly available services. In particular, it is prohibited to record, intercept, store messages or other types of interception or monitoring of messages and their associated data by persons other than the users or without the consent of the users concerned, unless regulated otherwise. This does not prevent the technical storage of data that are necessary for the transmission of messages, without prejudice to the principle of confidentiality.

Further to this, the undertaking company shall not be liable for the protection of transmitted messages if there is a possibility of their direct listening or unprotected acquisition at the place of transmission or at the place of reception.

However, this ban does not apply to temporary recording and storing of messages, as well as related Traffic Data if it is required:

- for the provision of value added services ordered by a subscriber or user;
- to prove a request to establish, change or withdraw the service; or
- to prove the existence or validity of other legal acts, which the subscriber, user or undertaking company has made.

Article 5 (3) of Directive No. 2002/58/EC of the European parliament and of the Council on concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) was implemented into Section 109 of the Act. Under Section 109 (8) of the Act: “*every person that stores or gains access to information stored in the terminal equipment of a user shall be authorised for that only if the user concerned has given his / her demonstrable consent. The obligation to obtain consent does not apply to law enforcement authorities and other state authorities. This shall not prevent any technical storage of data or access hereof for the sole purpose of the conveyance or facilitation of the conveyance of a communication by means of a network or if strictly necessary for the provider of an information society service to provide information society services if explicitly requested by the user.*”

Processing of cookies requires a demonstrable consent of the user. According to the opinion of the Office of Electronic Communication and Postal Services as the demonstrable consent according to the Act is considered such consent which met the conditions stipulated in Section 5 lit. a) of the Slovak Data Protection Act. In order for the consent to be freely given, access to services and features must not be conditional by the user's consent to the processing or storage of information through cookies. Access to the content, services or features on the website cannot be bound or conditioned by the granting such consent. Conditional use of the website by providing the user's consent with processing or storing information through cookies is a violation of Section 109 (8) of the Act.

Traffic Data

Traffic Data are data related to the user and to the specific transmission of information in the network and arising during this transmission, which are processed for the purposes of transmission of messages in the network or for invoicing purposes. The Traffic Data related to subscribers or users may not be stored and the undertaking company is required, after the end of a communication transmission, without delay, to destroy or make anonymous such Traffic Data, except as provided otherwise by the Act.

If it is necessary for the invoicing of the subscribers and network interconnection payments, the undertaking company is required to store the Traffic Data until the expiration of the period during which the invoice may be legally challenged or the claim for the payment may be asserted. The undertaking company is required to provide the Traffic Data to the Office for Electronic Communications and Postal Services or the court in the case of a dispute between undertaking companies or between an undertaking company and a subscriber. In the event of a complaint, alternative dispute resolution, out-of-court dispute resolution or legal proceedings, in particular disputes relating to network connection or invoicing, the undertaking company must retain Traffic Data until the expiry of the period for all legal remedies. The scope of the stored Traffic Data must be limited to the minimum necessary.

The undertaking company is further authorized to process Traffic Data and Location Data (as described below) to the necessary extent even without the user's consent for the purposes:

- network operations, services or networks and services;

- accounting for the provided service, invoicing and proof of entitlement to payment for the provided service in debt collection;
- dealing with questions, complaints and claims of users;
- prevention and detection of security incidents and illegal actions; or
- providing cooperation to authorized state authorities.

The provider of a publicly available service may process the Traffic Data of the subscriber or user for the purposes of marketing services or for the purpose of providing value added services only with his / her prior consent and only to the extent and during the time necessary for marketing services and providing value added services. The undertaking company is obliged to inform the subscriber or user before obtaining his / her consent about the type of Traffic Data, the purpose of processing Traffic Data and the time of processing of this data. The subscriber or user may at any time revoke their consent to the processing of Traffic Data for marketing purposes or to provide value added services.

Location Data

Location Data are data processed in the network or through the service that indicates the geographic location of the end device of the user of the publicly available service. The undertaking company may process the Location Data other than the Traffic Data which relates to the subscriber or the user of a public network or public service only if the data are made anonymous or the processing is done with consent of the user or subscriber of a public network or publicly available service, and in the scope and time necessary for the provision of the value added service or if the Act provides so. The undertaking company must, prior to obtaining consent, inform the subscriber or user of the Location Data other than Traffic Data which will be processed, on the type of Location Data to be processed, on the purpose and duration of the processing, and whether the data will be provided to a third party for the purpose of the provision of the value added service. The subscriber or user may revoke its consent for the processing of Location Data at any time. If the subscriber or user has agreed to the processing of Location Data other than Traffic Data for the provision of a value added service, the undertaking company is obliged to allow him / her to temporarily refuse the processing of such Location Data in a simple way and free of charge every time he / she connects to the network or every time he / she transmits a message. The processing of Location Data, as described in previous sentences, shall be limited to persons acting on behalf of an undertaking company providing public networks or publicly available services, or to persons of a third party providing a value-added service and must be limited to the necessary purposes of providing a value added service.

KEY CONTACTS

JUDr. Dr. Michaela Stessl
Country Managing Partner
T +421 2 59202 122
michaela.stessl@dlapiper.com

Eva Skottke
Senior Associate
T +421 2 59202 111
eva.skottke@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SLOVENIA

Last modified 17 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by the GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

The new Slovenian Data Protection Act (ZVOP-2) which implements certain aspects of the GDPR has been adopted in December 2022 and has entered into force on 26 January 2023. From thereon, data protection is regulated by three main legal acts: (i) ZVOP-2; (ii) GDPR and (iii) Slovenian Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences (*Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj*, Official Gazette no. 177/20; ZVOPOKD), which has entered into force on 31 December 2020 and implements Directive 2016/680. In relation to ZVOP-2, ZVOPOKD is considered lex specialis, therefore provisions of ZVOP-2 will not be used for questions specifically provided for and regulated by ZVOPOKD.

ZVOP-2 also regulates certain areas of data processing, not regulated by GDPR, namely:

- processing of personal data of deceased persons;
- processing of personal data in relation to carrying out activities outside of EU-law scope; and
- processing of personal data by the authorities of Slovenia when acting in areas of security and defence policy and carrying out intelligence and security activities.

Certain other Slovenian acts also regulate personal data processing, which is not set forth by GDPR, i.e.:

- Defence Act (*Zakon o obrambi*, Official Gazette no. 103/04 as amended from time to time and in force);
- Slovenian Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji*; Official Gazette no. 81/06 as in force);
- Attorneys Act (*Zakon o odvetništvu*, Official Gazette no. 18/93 as amended from time to time and in force);
- Classified Information Act (*Zakon o tajnih podatkih*; Official Gazette no. 50/06 as amended from time to time and in force);
- Electronic Communications Act (*Zakon o elektronskih komunikacijah*, Official Gazette no. 130/22 as in force);
- Minor Offences Act (*Zakon o prekrških*; Official Gazette no. 29/11 as amended from time to time and in force);
- Patients’ Rights Act (*Zakon o pacientovih pravicah*; Official Gazette no. 15/08 as amended from time to time and in force);
- Mass Media Act (*Zakon o medijih*; Official Gazette no. 110/06 as amended from time to time and in force);
- Banking Act (*Zakon o bančništvu*; Official Gazette no. 92/21 and 123/21 as in force);

- Public Procurement Act (*Zakon o javnem naročanju*; Official Gazette no. 91/15 as amended from time to time and in force);
- Employment Relationship Act (*Zakon o delovnih razmerjih*; Official Gazette no. 21/13 as amended from time to time and in force).

In accordance with Article 3(3) ZVOP-2, the above-listed acts are considered lex specialis in relation to ZVOP-2, meaning that provisions of ZVOP-2 will be applicable subsidiarily, when certain questions are not covered by the above-mentioned acts. Despite that, provisions of Articles 4-7 and 9-23 of GDPR would still apply *mutatis mutandis*, when such applicability is possible and appropriate (for instance in matters of threat to national security national legal provisions would prevail over the provisions of GDPR).

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "to the offering of goods or services" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "the monitoring of their behaviour" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

In addition to the above, provisions of ZVOP-2 (together with GDPR) will apply when:

- processing of personal data is carried out within the public sector of Slovenia (Article 4(1) ZVOP-2); or
- processing of personal data is carried out within private sector when the following conditions are met:
  - the processor and / or controller is established in Slovenia, even if the processing of personal data does not take place in Slovenian territory (Article 4(1) ZVOP-2); or
  - the processor and / or controller is established outside EU but carries out activities of “offering services and goods” to persons domiciled in Slovenia in relation to person data processing, irrespective of whether a payment of data subject is required or are in relation to monitoring of data subjects’ behaviour (Article 4(2) ZVOP-2).

DEFINITIONS

In accordance with Article 5(1) ZVOP-2, terms used in ZVOP-2 have the same meaning as terms defined by Article 4 GDPR.

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 5(1) ZVOP-2 in connection with Article 4 GDPR). A low bar is set for "**identifiable**" – meaning a personal identification number; and any other (by law) defined unique identifiers of individuals by means of which it is possible to collect or retrieve personal data from personal data files in which unique identifier are processed; and other similar signs which are used regularly or systematically for linking databases between different controllers or between two or several files within one controller; a name is not necessary – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person (Article 5(2-V.) ZVOP-2).

Online identifiers are expressly called out in Recital 30 GDPR, with IP addresses, cookies and RFID tags all listed as examples.

ZVOP-2 contains more restrictive rules for the processing of "**special categories**" of personal data (including data relating to race, religion and nationality (Article 6(5) ZVOP-2), genetics and biometrics (Articles 81-84 ZVOP-2)) and personal data relating **to criminal convictions and offences** (Article 10 ZVOP-2), which do not differentiate from provisions of Article 9-10 GDPR. Additionally, ZVOP-2 creates rules regulating personal data relating to deceased persons (Article 9 ZVOP-2). Such personal data may be processed by either data processors authorized by law, family members, any entities who have legal interest exercising their rights before Slovenian authorities or to whom the deceased had given their consent for such processing prior to their passing. Provisions of Article 9 ZVOP-2 apply for 20 years after individuals passing away, unless otherwise provided by law.

ZVOP-2 together with GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation, or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "alone or jointly with others, determines the purposes and means of the processing of personal data" (Article 5(1) ZVOP-2 in connection with Article 4 GDPR). The processor "processes personal data on behalf of the controller", acting on the instructions of the controller. In contrast to the previous law, the ZVOP-2 together with GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Slovenian Data Protection Authority *(Informacijski pooblaščenec)* can be contacted as follows:

Informacijski pooblaščenec
Dunajska cesta 22, 1000 Ljubljana
Slovenia / Europe

Phone number: +386 1 230 97 30

Enail: gp-ip@ip-rs.si

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- It is a public authority;
- Its core activities consist of processing operations which, by virtue of their nature, scope, or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- Its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2) GDPR), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5) GDPR) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6) GDPR).

It should be noted that ZVOP-2 provides for two other requirements for appointment of DPOs, namely: (a) legal capacity and (b) that the person has not been sentenced to a minimum term of imprisonment of six months or has not been the subject of a final conviction for a criminal offence relating to the misuse of personal data. Additional conditions also vary depending on whether the DPO works in a public authority, public sector (other than public authority) or in the private sector.

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1) GDPR), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks (Article 38(3) GDPR).

The specific tasks of the DPO, set out in GDPR, include (Article 39 GDPR):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities,
- awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

In accordance with Article 48 ZVOP-2, DPO performs tasks listed in Article 39 GDPR, and specifically, provides advice on risk assessments regarding the security of personal data related to all processing of personal data in databases which is carried out by the controller or processor to whom they are assigned.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5 GDPR):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant, and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and

- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "*accountability principle*"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to demonstrate compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1) GDPR):

- with the consent of the data subject (where consent must be "freely given, specific, informed and unambiguous", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9 GDPR), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to Article 6 GDPR basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and
- social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally
- incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1) GDPR.

ZVOP-2 includes further conditions and limitations for processing with regard to processing genetic data, biometric data and data related to ethnicity and race. Part 13 of Patients’ Rights Act sets forth further limitations with regard to processing health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10 GDPR).

In accordance with Article 10(2) ZVOP-2, processing of personal data relating to criminal convictions and offences is only allowed if it so prescribed by the law, including:

- further specification of the purpose of such processing, which must be in the public interest;
- types of data which can be processed;
- data subjects;
- entities / individuals to whom such data can be disclosed;
- specification of purpose of disclosure including its limitations;
- data retention limits; and
- measures ensuring lawful and fair processing.

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider ascertaining whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4) GDPR). These include:

- any link between the original purpose and the new purpose;
- the context in which the data have been collected;
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects; and
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Additionally, in accordance with Article 7 ZVOP-2 processing of personal data for secondary purposes is only possible if the processing is:

- in public interest;
- done by authorities in the public sector, when carrying out their legal obligations;
- allowed based on the law; and
- done in accordance with Article 6(4) GDPR.

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent, and easily accessible form, using clear and plain language (Article 12(1) GDPR).

The following information must be provided (Article 13 GDPR) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14 GDPR) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15 GDPR)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16 GDPR)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17 GDPR)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18 GDPR)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20 GDPR)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21 GDPR)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22 GDPR)

Automated decision making (including profiling) "which produces legal effects concerning [the data subject] … or similarly significantly affects him or her" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorised by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

ZVOP-2 adds only specifications to the general processing requirements. The age for consent of children for the purposes of Article 8(1) GDPR is 15 years, unless general terms and conditions of the processor set forth a higher age limit. If consent is given by children under age 15, it is only valid if it is approved by the child’s parent or legal guardian.

ZVOP-2 sets forth further requirements regarding special areas of personal data processing:

a. processing of personal data for the purposes of scientific research, statistical research and for historic / archival purposes;

   For such purposes, processing of personal data (including special categories of personal data) is allowed by organizations and / or researchers if in the course of their activities they apply ethical principles and methodology in accordance with their field of research.

   Processing is permitted if:
   - it is permitted by law; or
   - the data subject has not prohibited processing of his / her personal data for such research purposes; or
   - the data subject has given written consent for the processing of his / her personal data if personal data means professional secrecy.

     Furthermore, research organizations and / or researchers can access certain types of personal data if they fulfil specific conditions and requirements.

b. processing of personal data in the context of exercising freedom of speech;

   Under certain circumstances, especially if personal data has already been publicly disclosed, if individuals cannot expect protection of his / her privacy or the public interest exists, personal data can be published and processed when exercising freedom of speech.

c. video surveillance;

If authorized persons want to introduce video surveillance, they must publish a notification. Apart from requirements provided for in Article 13(1) GDPR, the controller must publish some additional information either on the site or on websites. If such notification is published, it can be subsumed that the individual has been informed about video surveillance. Videos can be stored in accordance with Article 5 GDPR for up to 1 year since the video has been made.

In any case, video surveillance is prohibited in elevators, toilets, hotel rooms, changing rooms and any premises in which the individual expects higher level of protection of his / her privacy.

Some further conditions and requirements are set forth for video surveillance in workplaces, business premises, public transport, or public places.

d. processing of biometric and genetic data;

Processing of biometric and genetic data is very restricted and is only allowed if certain conditions / circumstances in accordance with ZVOP-2 are met.

e. evidence of entrance and exists in business premises;

f. publicly available databases;

g. data processing of contact data and personal documents of employees and / or other individuals who are key contacts for conducting a business (both in the private and public sector).

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein, and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44 GDPR).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1) GDPR).

Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Japan, Republic of Korea, United Kingdom (under the GDPR and the Law Enforcement Directive), Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules and standard contractual clauses. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise, or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or

g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals, or administrative authorities of countries outside the EU (Article 48 GDPR) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

No general additional requirements relating to transfers are introduced by ZVOP-2.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 GDPR states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However, the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. The pseudonymization and encryption of personal data;
b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

ZVOP-2 provides no general additional requirements in relation to security measures. In the context of archiving, scientific or historical research purposes or statistical purposes, the ZVOP-2 sets out specific rules including anonymization or pseudonymization requirements.

Security measures are also detailed for each special regime but resemble the GDPR.

However, Article 22 ZVOP-2 provides additional requirements regarding data security by prescribing the so‑called "processing log" (dnevnik obdelave), namely by specifying:

- who must ensure processing logs;
- for which processing activities;
- what the processing log must contain;
- for which purposes the processing log can be used; and
- data retention periods in processing logs.

Article 23 ZVOP-2 specifies data security requirements in the field of special processing. These requirements apply to particularly risky information systems processing large amounts of sensitive, confidential, or otherwise protected data, including special categories of personal data.

Article 21 ZVOP-2 also includes provisions related to the protection of personal data in proceedings related to such personal data.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed*" (Article 4 GDPR).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34 GDPR).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2) GDPR).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3) GDPR).

Controllers are also required to keep a record of all data breaches (Article 33(5) GDPR) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

In relation to data breaches, in Article 23 ZVOP-2 regulates data security in the field of special processing, which also involves reporting breaches. This article specifies that for certain information systems, the provisions on security requirements and reporting incidents from the Information Security Act (*Zakon o informacijski varnosti*) apply mutatis mutandis. These provisions concern essential service providers if the controller is not obliged to implement measures under the Information Security Act for these processing activities. Localization rules apply exist in case of special processing of personal information within information systems in which processing of the following categories of personal data is carried out: personal data specified in the laws governing administrative internal affairs, financial administration, citizenship, the Slovenian Intelligence and Security Agency, defence, healthcare, mandatory health insurance, the exercise of rights deriving from public funds, and criminal and minor offence records. Such data records must be kept within the territory of the Republic of Slovenia.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.

The highest fines (Article 83(5) GDPR) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4) GDPR) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate, and dissuasive (Article 83(1) GDPR).

Fines can be imposed in combination with other sanctions.

It should be noted that the Slovenian Information Commissioner (*Informacijski pooblaščenec*) can impose fines on the basis of ZVOP-2.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58 GDPR) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- Any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1) GDPR) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- Data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80 GDPR).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77 GDPR).

All natural and legal persons, including individuals, controllers, and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78 GDPR).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79 GDPR).

No general additional requirements are inserted in ZVOP-2.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47 GDPR). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to

incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3) GDPR).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR.

As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Direct marketing by means of electronic communications is regulated by the Consumer Protection Act (Zakon o varstvu potrošnikov, Official Gazette 130/22), the Electronic Commerce Market Act (*Zakon o elektronskem poslovanju na trgu*, Official Gazette 96/09 as amended from time to time and in force), the Electronic Communications Act (*Zakon o elektronskih komunikacijah*, Official Gazette no. 130/22) and ZVOP-2.

The consent of an individual is required for the purposes of electronic marketing. Direct marketing is allowed where the "similar service / product" exemption applies, however customers must be given clear and distinct opportunity to refuse the use of their electronic mail address at the time of the collection of these contact details, and on the occasion of every message in the event that the customer has not initially refused such use. Additionally, the sending of electronic mail for the purposes of direct marketing, which disguises or conceals the identity of the sender, or is sent without a valid address, is prohibited.

ONLINE PRIVACY

Traffic data

Traffic Data must be erased or made anonymous as soon as it is no longer needed for the purpose of the transmission of a communication, except in cases where a longer period of retention is statutory allowed. Nevertheless, an operator may, until complete payment for service is made but no later than by expiry of the limitation period, retain and process traffic data required for the purposes of calculation and of payment relating to interconnection.

Location data

Location Data may only be processed for the purposes of providing the value-added service and when it is made anonymous, or with the prior consent of the user or subscriber, who may withdraw this consent at any time. Prior to issuing consent, a user or subscriber must be informed on (i) the possibility of refusing consent, (ii) the type of data to be processed, (iii) the purpose and duration of processing, and (iv) the possibility of the transmission of location data to a third party for the purpose of providing the value-added service.

Cookie compliance

The Electronic Communications Act (ZEKom-2) provides rules on the usage of cookies and similar technology for data storage.

Pursuant to ZEKom-2 the retention of information or the gaining of access to information stored in a subscriber’s or user’s terminal equipment (cookies) is only permitted if the subscriber or user gave their informed consent after having been given clear and comprehensive information about the information manager and the purpose of the processing of this information. However, an exception is provided in case of carrying out the transmission of a communication over an electronic communications network, or if this is strictly necessary for provision of service of information society explicitly requested by the subscriber or user.

KEY CONTACTS

Dr. Jasna Zwitter-Tehovnik
Partner
T +43 1 531 78 1042
jasna.zwitter-tehovnik@dlapiper.com

Domen Brus
Senior Associate
T +43 1 531 781848
domen.brus@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SOUTH AFRICA

Last modified 17 January 2024

LAW

The right to privacy is recognized as a fundamental human right in the Bill of Rights of the Constitution of the Republic of South Africa and is protected in terms of the Constitution and the common law. This right to privacy is not absolute and may be limited where it is reasonable and justifiable to do so.

The Protection of Personal Information Act 4 of 2013 (POPIA) came into effect on 1 July 2020 but was subject to a one year grace period which ended on 30 June 2021. POPIA specifically regulates the processing of personal information that is entered into a record pertaining to natural living persons as well as existing legal persons.

DEFINITIONS

Definition of personal data

"Personal information" is defined in POPIA as information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing, juristic person, including:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin; color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief; culture, language and birth of the person;
- Information relating to the education, medical, financial, criminal or employment history of the person;
- Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- The biometric information of the person;
- The personal opinions, views or preferences of the person;
- Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- The views or opinions of another individual about the person; and
- The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

POPIA applies to the processing of personal information entered in a record by or for a responsible party / data controller that is domiciled in South Africa and that makes use of automated or non-automated means to process the personal information. It would also apply if the responsible party is not domiciled in South Africa but makes use of automated or non-automated means in South Africa unless those means are used only to forward personal information through South Africa.

POPIA does not apply to the processing of personal information:

- In the course of a purely personal or household activity;

- That has been de-identified to the extent that it cannot be re-identified again;
- By or on behalf of the State with regard to national security, defense or public safety, or the prevention, investigation or proof of offenses; or for the purposes of the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in specific legislation for the protection of such personal information;
- For exclusively journalistic purposes by responsible parties who are subject to, by virtue of office, employment or profession, a code of ethics that provides adequate safeguards for the protection of personal information;
- Solely for the purposes of journalistic, literary or artistic expression to the extent that such exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression;
- By Cabinet and its committees, the Executive Council of a province and a Municipal Council of a municipality;
- For purposes relating to the judicial functions of a court referred to in section 166 of the Constitution; and
- Under circumstances that have been exempted from the application of the conditions for lawful processing by the Information Regulator in certain circumstances.

Definition of sensitive personal data

Special personal information is information concerning religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information and criminal behavior (to the extent that such information relates to the alleged commission of an offense or any proceedings in respect of any offence allegedly committed, or the disposal of such proceedings).

Subject to certain prescribed exceptions, the processing of special personal information without the consent of the data subject is generally prohibited under POPIA.

NATIONAL DATA PROTECTION AUTHORITY

The Information Regulator has established an Enforcement Committee and initiates investigations into various possible violations of POPIA. There is scrutiny by the Information Regulator into security compromises including the establishment of a security compromise register. These activities are in line with the powers, duties and functions of the office of the Information Regulator which include providing education regarding the protection and processing of personal information; monitoring and enforcing compliance with the provisions of POPIA; consulting with interested parties and acting as mediator; receiving, investigating and attempting to resolve complaints; issuing enforcement notices and codes of conduct; and facilitating cross-border cooperation.

REGISTRATION

Data protection officers (referred to in POPIA as "**information officers**") must be registered with the Information Regulator.

Responsible parties are required to obtain prior authorization from the Information Regulator before processing personal information in certain circumstances prescribed in section 57 of POPIA, for example, where special personal information or personal information of children is transferred to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information and where information on criminal behavior or unlawful or objectionable conduct is processed on behalf of third parties. Prior authorization is also required when processing personal information for the purposes of credit reporting or when processing unique identifiers for a purpose other than the purpose for which it was originally collected and linking it with personal information processed by other third parties. Responsible parties are not otherwise required to register their processing of personal information.

The prior authorization requirements in POPIA came into effect on 1 February 2022. This means that all responsible parties (i.e. data controllers) that conduct processing activities that are subject to prior authorization need to submit an application for prior authorization and will need to cease such processing activities until such time as prior authorization is obtained.

DATA PROTECTION OFFICERS

Data protection officers (referred to in POPIA as "**information officers**") must be registered with the Information Regulator. The duties and responsibilities of a responsible party's information officer are set forth in POPIA and include encouraging and ensuring compliance with POPIA; dealing with any requests made to that responsible party in terms of POPIA; and working with

the Information Regulator in respect of investigations by the Information Regulator in relation to that responsible party. The Regulations to POPIA, among other things, further provide that the information officer must ensure that a compliance framework is developed, implemented, monitored and maintained, and that a personal information impact assessment is conducted to ensure that adequate measures and standards for the protection of personal information exist.

COLLECTION & PROCESSING

"Processing" of information is defined in POPIA as any operation or activity or any set of operations, whether or not by automatic means,concerning personal information, including:

- The collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- Dissemination by means of transmission, distribution or making available in any other form; and
- Merging, linking, as well as blocking, degradation, erasure or destruction of information.

POPIA prescribes the following eight conditions for lawful processing of personal information:

- **Accountability**: The responsible party must comply with all the conditions for lawful processing.
- **Purpose specification**: Personal information must only be collected for a specific, explicitly defined lawful purpose related to a function or activity of the responsible party.
- **Processing limitation**: Processing must be justified on a ground recognized under POPIA (e.g. consent / legitimate interests of the data subject, responsible party or the third party to whom the information is supplied).
- **Further processing limitation**: Processing must be in accordance with or compatible with the purpose for which it was initially collected subject to limited exceptions.
- **Information quality**: Steps must be taken to ensure that the information is complete, accurate, not misleading and updated where necessary.
- **Openness**: Notification requirements must be complied with when collecting personal information.
- **Security safeguards**: Appropriate, reasonable technical and organizational measures must be implemented and maintained to prevent loss of, damage to or unauthorized destruction of or unlawful access to personal information.
- **Data subject participation**: Data subjects have the right to request details of the personal information that a responsible party holds about them and, in certain circumstances, request access to such information.

TRANSFER

POPIA caters for two scenarios relating to the transfer of personal information, namely where a responsible party in South Africa sends personal information to another country to be processed and where a responsible party in South Africa processes personal information that has been received from outside South Africa.

Receiving personal information from other countries

The requirements for the processing of personal information prescribed in POPIA will apply to any personal information processed in South Africa, irrespective of its origin.

Sending personal information to other countries for processing

A responsible party in South Africa may not transfer personal information to a third party in another country unless:

- The recipient is subject to a law, binding corporate rules or a binding agreement which:
  - Upholds principles for reasonable processing of the information that are substantially similar to the conditions contained in POPIA; and
  - Includes provisions that are substantially similar to those contained in POPIA relating to the further transfer of personal information from the recipient to third parties who are in another country;
- The data subject consents to the transfer;
- The transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject’s request; or

- The transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject’s request; or
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party, or the transfer is for the benefit of the data subject and:
    - It is not reasonably practicable to obtain the consent of the data subject to that transfer; and
    - If it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

SECURITY

Section 19 of POPIA places an obligation on a responsible party to secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss, damage to, or unauthorised destruction of, and unlawful access to, personal information.

To comply with this obligation, the responsible party must take reasonable measures to do all of the following:

- Identify all reasonably foreseeable internal and external risks to personal information under its control;
- Establish and maintain appropriate safeguards against the risks identified;
- Regularly verify that the safeguards are effectively implemented; and
- Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

The responsible party must also have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

BREACH NOTIFICATION

In terms of section 22 of POPIA, where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorized person, the responsible party must notify the Information Regulator and the data subject, unless the identity of such data subject cannot be established.

The notification must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party’s information system.

The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offenses or the Information Regulator determines that notification will impede a criminal investigation by the public body concerned and must be in writing and communicated to the data subject in a prescribed manner.

The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including all of the following:

- A description of the possible consequences of the security compromise;
- A description of the measures that the responsible party intends to take or has taken to address the security compromise;
- A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
- If known to the responsible party, the identity of the unauthorized person who may have accessed or acquired the personal information.

The Information Regulator may direct a responsible party to publicize, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Information Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

An operator / data processor is not required to notify the Information Regulator or data subjects where there are reasonable grounds to believe that there has been a data breach. It must, however, notify the responsible party / data controller of the suspected data breach.

ENFORCEMENT

Any person may submit a complaint to the Information Regulator alleging non-compliance with POPIA. The Information Regulator may also initiate an investigation into interference with the protection of personal information.

Upon receipt of a complaint, the Information Regulator may, inter alia, conduct a pre-investigation or full investigation of the complaint, act as conciliator, refer the complaint to another regulatory body if the Information Regulator considers that the complaint falls more properly within the jurisdiction of the other regulatory body, or decide to take no further action.

The Information Regulator's powers, for purposes of investigating a complaint include the power to summons and enforce the appearance of persons before the Information Regulator to give evidence or produce records or things; enter and search the premises occupied by a responsible party; and conduct interviews and inquiries.

If the Information Regulator is satisfied that a responsible party has interfered or is interfering with the protection of the personal information of a data subject it my issue an enforcement notice prescribing action to be taken by the responsible party to remedy the situation.

A responsible party who fails to comply with an enforcement notice is guilty of an offense and is, liable, on conviction, to a fine or imprisonment (or both) for a period of no longer than ten years (in terms of section 107), or alternatively to an administrative fine (in terms of section 109). Currently, the maximum fine under sections 107 and 109 of POPIA is R10 million.

Section 99 also makes provision for a civil action for damages resulting from non-compliance with POPIA. In order to succeed in such a claim the complainant would need to prove all the elements of a delict: wrongful conduct, causation, fault (intent / negligence) and harm. The data subject would need to prove the quantum of the damages that s/he seeks.

ELECTRONIC MARKETING

Direct marketing by means of unsolicited electronic communications is regulated by POPIA whereby the opt-in regime has taken effect. Accordingly, under POPIA, the processing of a data subject's personal information for the purposes of direct marketing by means of unsolicited electronic communications is prohibited unless the data subject has given its consent, or the email recipient is an existing customer of the responsible party. A responsible party may only approach a data subject once in order for the data subject to opt in to receive marketing information. The Regulations to POPIA contain a prescribed form to be used when seeking this opt-in.

When sending emails to a data subject who is an existing customer:

a. the responsible party must have obtained the details of the data subject through a sale of a product or service;
b. the marketing should relate to its own similar products or services; and
c. the data subject must have been given a reasonable opportunity to opt out, free of charge, of the use of its personal information for marketing when such information was collected and on each occasion that marketing information is sent to the data subject, if the data subject has not initially refused the use of the personal information for electronic marketing purposes.

Direct marketing that is not by electronic communications (i.e. telephone or in-person marketing) continues to be regulated by the Consumer Protection Act, which requires the consumer to have an opportunity to opt out of receiving direct marketing.

ONLINE PRIVACY

There are no sections of POPIA that expressly regulate privacy in relation to cookies and location data. These issues may be dealt with in subsequent regulations or codes of conduct to be issued by the Information Regulator.

KEY CONTACTS

DLA Piper

Monique Jefferson
Director
T +27 11 302 0853
monique.jefferson@dlapiper.com

Justine Katz
Associate
T +27 (0)11 302 0846
justine.katz@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SOUTH KOREA

Last modified 19 January 2024

LAW

The main laws that apply to the handling of data about individuals are the Personal Information Protection Act (“**PIPA** ”) (amended in September 2023) and the Act on the Use and Protection of Credit Information (“**CIA**”).

Prior to 5 August 2020, the Act on Promotion of Information and Communications Network Utilization and Data Protection (“**Network Act**”) contained data protection-related provisions applicable to Online Service Providers (OSPs), which are (i) telecommunications service providers registered under the Telecommunications Business Act or (ii) a person who provides information or mediates the provision of information for profit by using services provided by a telecommunications service provider. Most organisations that operate websites / apps (except for non-profit organisations) as well as network operators are OSPs. However, most of these provisions were moved to the PIPA (Chapter 6, Special Rules on Processing of Personal Information by Online Service Providers), pursuant to an amendment to the Network Act and the PIPA that went into effect on 5 August 2020.

In 2023, the PIPA was further amended in keeping up with the principle of “same conduct – same regulation” for all personal data controllers by repealing special provisions that previously only applied to OSPs. The Amended PIPA has become effective from 15 September 2023, with certain exceptions such as the right of portability, where the effective date is yet to be determined. On 23 November 2023, the Personal Information Protection Commission (“**PIPC** ”) which is tasked with enforcing the PIPA proposed an amendment to the Enforcement Decree of the PIPA to provide the subordinate details of the PIPA amendments.

DEFINITIONS

Definition of personal data

Under PIPA, “personal information” means information relating to a living individual that constitutes any of the following:

a. Information that identifies a particular individual by his / her full name, resident registration number, image, etc.
b. Information which, even if by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual (in this case, whether or not there is ease of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual such as likelihood that the other information can be procured)
c. Information under items (a) or (b) above that is pseudonymised in accordance with the relevant provisions and thereby becomes incapable of identifying a particular individual without the use or combination of information for restoration to the original state (referred to as “pseudonymised information”).

Definition of sensitive personal data

Under the PIPA, “sensitive information” is defined as personal information concerning an individual’s ideology, faith, labor union

membership, political views or membership in a political party, health or medical treatment information, sexual orientation, genetic information, criminal records and biometric data for the purpose of uniquely identifying a natural person and race / ethnic information. Sensitive information can be processed if (a) such processing is required or permitted by a statute, or (b) the consent of the data subject is separately obtained.

Definition of Unique Identification personal data

Under the PIPA, “unique identification information” is defined to be Resident registration number (“**RRN** ”), driver’s license number, passport number, and foreigner registration number. Other information, apart from RRNs, can be processed if (a) such processing is required or permitted by statute, or (b) the consent of the data subject is separately obtained. RRN can only be processed based on a legal basis, irrespective of whether consent to the processing is obtained from the data subject.

NATIONAL DATA PROTECTION AUTHORITY

The PIPC is in charge of the enforcement of PIPA.

The PIPC shall perform the following work:

1. Matters concerning the improvement of law relating to personal information protection;
2. Matters concerning the establishment or execution of policies, systems or plans relating to personal information protection;
3. Matters concerning investigation into infringement upon the rights of data subjects and the ensuing dispositions;
4. Handling of complaints or remedial procedures relating to personal information processing and mediation of disputes over personal information;
5. Exchange and cooperation with international organizations and foreign personal information protection agencies to protect personal information;
6. Matters concerning the investigation and study, education and promotion of law, policies, systems and status relating to personal information protection;
7. Matters concerning the support of technological development and dissemination relating to personal information protection and nurturing of experts; and
8. Matters specified as the work of the PIPC by the PIPA or other statutes.

REGISTRATION

Under PIPA, there is no general rule regarding the registration of personal data controller, however, a public institution which manages a personal information file (i.e. collection of personal information) shall register the following with the PIPC. A “ public institution” in this context refers to any government agency or institution.

- name of the personal information file;
- basis and purpose of operation of the personal information file;
- items of personal information which are recorded in the personal information file;
- the method to process personal information;
- period to retain personal information file;
- person who receives personal information generally or repeatedly; and
- other matters prescribed by the Presidential Decree.

The Presidential Decree of PIPA stipulates that the followings also shall be registered with the PIPC:

- the name of the institution which operates the personal information file;
- the number of subjects of the personal information included in the personal information file;
- the department of the institution in charge of personal information processing;

- the department of the institution handling the data subjects’ request for inspection of personal information; and
- the scope of personal information inspection of which can be restricted or rejected and the grounds therefore only “public institutions” are required to register with the PIPC.

DATA PROTECTION OFFICERS

Under PIPA, every personal data controller (which means any person, any government entity, company, individual or other person that, directly or through a third party, controls and / or processes personal information in order to operate personal information files as part of its activities) must designate a chief privacy officer (“**CPO**”) who must be an employee or executive of the company.

The CPO’s obligations under the PIPA are as follows:

- establishing and implementing plans for the protection of personal information;
- performing periodic investigations and improving the status and practices of the processing of personal information;
- handling complaints and dealing with damage pertaining to the processing of personal information;
- establishing internal control systems for preventing leakage, misuse and abuse of personal information;
- establishing and implementing training sessions for the protection of personal information;
- protecting, managing, and monitoring personal information files;
- establishing, amending, and implementing a personal information processing policy;
- managing materials concerning the protection of personal information; and
- destroying personal information for which the purpose of processing has been achieved or for which the retention period has expired.

The Proposed Enforcement Decree of the PIPA lays the grounds for the CPO to independently perform his / her duties. Under the Proposed Enforcement Decree, a personal data controller must (i) guarantee the CPO’s access to all information in relation to the processing of personal information, (ii) establish a system for the CPO’s direct reporting to the representative and the board of directors at least once a year, (iii) provide the CPO with human and material resources by creating an organizational structure suitable for the performance of duties, and (iv) prohibit a situation where the CPO is placed at a disadvantage by reason of non-compliance with unreasonable instructions.

Personal data controllers that meet certain criteria are required to designate a CPO with (i) at least three years of experience in personal information protection, and (ii) a combined career of at least six years in personal information protection, data protection, and information technology. More specifically, the obligation to designate a CPO with the foregoing qualifications is applicable to an entity whose annual sales revenue or income amounts to at least KRW 150 billion, and (i) processes sensitive information or unique identification information of at least 50,000 data subjects, or processes personal information of at least 1 million data subjects; (ii) is a school under the Higher Education Act with at least 10,000 enrolled students as of December 31 of the immediately preceding year; (iii) is a tertiary hospital under the Medical Service Act; or (iv) is a public institution operating a personal information processing system which meets the standards set by the PIPC.

There are no nationality or residency requirements for the CPO. In the event that a CPO is not designated, the personal information processing entity may be subject to a maximum administrative fine of KRW 10 million under the PIPA.

COLLECTION & PROCESSING

Under the PIPA, there must be a specific legitimate basis for collection and use of personal information, with the most representative basis being the data subject's consent. As a result, in principle, the explicit consent of data subjects must be obtained before processing their personal information. However, the data subjects' consent is not required in cases where the processing of personal information is prescribed by a statute or where it is necessary for an entity to process personal information in order to comply with its legal obligations.

Exceptions to the general rule above which are applicable to personal data controller are as follows:

- where special provisions exist in other statutes or it is unavoidable due to obligations under statutes or regulations;

- where it is unavoidable for a public institution’s performance of work under its jurisdiction as prescribed by statutes or regulations, etc;
- where it is necessary to perform an agreement entered into with a data subject or to take measures as requested by a data subject in the course of executing such agreement;
- where it is deemed manifestly necessary for the protection, from imminent danger, of life, bodily and property interests of a data subject or a third party;
- where it is necessary to attain the legitimate interests of a personal data controller, the interest of which is manifestly superior to the rights of the data subject. In such cases, processing shall be allowed only to the extent the processing is substantially related to the legitimate interests of the personal information controller and does not go beyond a reasonable scope.
- where it is urgently necessary for public safety and security, public health, etc.

While one consent form may be used, separate consents must be obtained respectively for each type of processing activity (e.g. collection and use, third party provision) and for different types of personal information (e.g. unique identification information and sensitive information).

Under the PIPA, data subjects must be informed of, and provide their consent to, the following matters before their personal information is collected and / or used:

- the purpose of the collection and use;
- the items of personal information that will be collected;
- the duration of the possession and use of the personal information; and
- the fact that the data subject has a right to refuse to give consent and the negative consequences or disadvantages that may result due to any such refusal.

The processing of the RRN (which is a type of unique identification information) is prohibited even with the consent of the data subject unless the processing is explicitly required or permitted under a statute.

If the data subject is under the age of 14, the consent of their legal guardian must be obtained.

TRANSFER

As a general rule, a personal data controller may not provide personal information to a third party without obtaining the prior opt in consent of the data subject.

Exceptions to the general rule above apply in the following cases:

- where there exists special provisions in any Act or it is necessary to fulfil an obligation imposed by or under any Act and subordinate statute;
- where it is necessary for a public institution to perform its affairs provided for in any Act and subordinate statute, etc;
- where it is deemed manifestly necessary for the protection of life, bodily and property interests of a data subject or a third party where imminently endangered; and
- where it is urgently necessary for the public safety and security, public health, etc.

Under the PIPA, a personal data controller must obtain consent after it notifies the data subject of:

- recipient of personal information;
- purposes for which the recipient of personal information uses such information;
- particulars of personal information to be provided;
- period during which the recipient retains and uses personal information;
- the fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent.

When a business transfer occurs, the personal data controller may transfer personal information without consent; provided that it must provide its data subjects a chance to opt out by providing a notice of:

- expected personal information transfer;

- contact information of the recipient of the personal information, including the name, address, telephone number and other contact details of the recipient; and
- means and process by which the data subjects may refuse to consent to the transfer of personal information.

In addition to the restrictions set out above, consent must be received as a general rule for the cross-border transfer of personal information under the PIPA, however, consent need not be received in the following cases:

- where there are special provisions on cross-border transfers under laws, treaties or other international agreements;
- where delegation of processing or storage is necessary for the execution and performance of agreements with data subjects and such details are disclosed in the privacy policy or notified to the data subjects via email, etc;
- where the recipient of personal information has taken all necessary measures, such as authentication and safety measures required by the PIPC, such as ISMS-P; or
- where the countries or international organizations that personal information is transferred to are recognized by the PIPC as having an adequate level of protection.

While this exemption from the overseas consent requirement was only applicable to OSPs, the amended PIPA now applies this exemption to all personal data controllers.

When obtaining consent for cross-border transfers, personal data controllers must notify the following:

- specific information to be transferred overseas;
- destination country;
- date, time, and method of transmission;
- name and the contact information of the third party;
- third party's purpose of use of the personal information and the period of retention and usage; and
- method and procedure for rejecting the cross-border transfer and the consequences thereof.

SECURITY

Under the PIPA, every personal data controller must, when it processes personal information of a data subject, take the following technical and administrative measures in accordance with the guidelines prescribed by the Presidential Decree to prevent loss, theft, leakage, alteration, or destruction of personal information:

- establishment and implementation of an internal control plan for handling personal information in a safe way;
- installation and operation of an access control device, such as a system for blocking intrusion to cut off illegal access to personal information;
- measures for preventing fabrication and alteration of access / log records;
- measures for security including encryption technology and other methods for safe storage and transmission of personal information; and
- measures for preventing intrusion of computer viruses, including installation and operation of vaccine software, and other protective measures necessary for securing the safety of personal information.

The PIPA provides detailed measures to be taken by the personal data controller in its subordinate regulations.

BREACH NOTIFICATION

In the event of a personal information leakage, the personal data controller must notify the affected data subjects within 72 hours of becoming aware of the leakage. The data controller must also report to the regulator within 72 hours if: (i) personal information of 1,000 or more data subjects has been leaked, (ii) sensitive information or unique identification information has been leaked, or (iii) personal information has been leaked through unauthorized access from the outside. However, no regulatory reporting is needed if the data controller is able to take measures to significantly reduce the possibility of infringement of the rights and interests of the affected data subjects, such as retrieving or deleting the compromised personal information.

ENFORCEMENT

The competent authorities may request reports on the handling of personal information, and also may issue recommendations or orders if a personal data controller violates the PIPA. Non-compliance with a request or violation of an order can result in fines, imprisonment, or both.

For example, PIPC, the supervising authority, can issue a corrective order in response to any breach of an obligation not to provide personal information to a third party. Breach of a corrective order leads to an administrative fine of not more than KRW 30 million. Prior to issuing a corrective order, PIPC may take an incremental approach and instruct, advise and make recommendations to the personal data controller. On the other hand, where personal information has been transferred to a third party without the consent of the data subject and in the absence of exceptional circumstances, both the transferor and the transferee (if it received the personal information knowing that the data subject had not given consent) can be subject to criminal sanctions (imprisonment of up to 5 years or a criminal fine of up to KRW 50 million).

Punitive damages

In instances of data breaches caused by the personal data controller's intentional act or negligence, the personal data controller may be liable for up to five times the damages suffered.

ELECTRONIC MARKETING

Under the Network Act, anyone who intends to transmit an advertisement by electronic transmission media must receive the explicit consent of the individual, but if the individual either withdraws consent or does not give consent, then an advertisement for profit may not be transmitted.

In addition, the transmitter of advertisement information for profit must disclose the following information specifically within the advertisement:

- the identity and contact information of the transmitter; and
- instructions on how to consent or withdraw consent for receipt of the advertisement information.

A person who transmits an advertisement shall not take any of the following technical measures:

- a measure to avoid or impede the addressee's denial of reception of the advertising information or the revocation of his consent to receive such information;
- a measure to generate an addressee's contact information, such as telephone number and electronic mail address, automatically by combining figures, codes, or letters;
- a measure to register electronic mail addresses automatically with intent to transmit advertising information for profit, and various measures to hide the identity of the sender of advertising information or the source of transmission of an advertisement.

ONLINE PRIVACY

Cookie, logs, IP information, etc. may also be regulated by the PIPA as personal information, if combined with other information may enable the identification of a specific individual person easily.

The protection of location information is governed by the provisions of the Act on the Protection, Use, etc. of Location Information (“**LBS Act**”).

Under the LBS Act, any person who intends to collect, use, or provide location information of a person or mobile object shall obtain the prior consent of the person or the owner of the object, unless:

- there is a request for emergency relief or the issuance of a warning by an emergency rescue and relief agency;
- there is a request by the police for the rescue of the person whose life or physical safety is in immediate danger, or there exist special provisions in any Act.

Under the LBS Act, any person (entity) who intends to provide services based on location information (“Location-based Service Provider”) shall report to the Korea Communications Commission (“**KCC**”). Further, any person

(entity) who intends to collect location information and provide the collected location information to Location-based Service Providers (“Location Information Provider”) shall obtain a license from the KCC.

If a Location Information Provider intends to collect personal location information, it must specify the following information in its service agreement, and obtain the consent of the subjects of personal location information:

- name, address, phone number and other contact information of the Location Information Provider;
- rights held by the subjects of personal location information and their legal agents and methods of exercising the rights;
- details of the services the Location Information Provider intends to provide to Location-based Service Providers;
- grounds for and period of retaining data confirming the collection of location information; and
- methods of collecting location information.

If a Location-based Service Provider intends to provide location-based services by utilizing personal location information provided by a Location Information Provider, it must specify the following information in its service agreement, and obtain the consent of the subjects of personal location information:

- name, address, phone number and other contact information of the Location-based Service Provider;
- rights held by the subjects of personal location information and their legal agents and methods of exercising the rights;
- details of the location-based services;
- grounds for and period of retaining data confirming the use and provision of location information; and
- matters concerning notifying the personal location information subject of the provision of location information to a third party as below.

If a Location-based Service Provider intends to provide location information to a third party, in addition to the above, it must notify the subjects of personal location information of the third party who will receive the location information and the purpose of this provision.

KEY CONTACTS

Kim and Chang
www.kimchang.com/

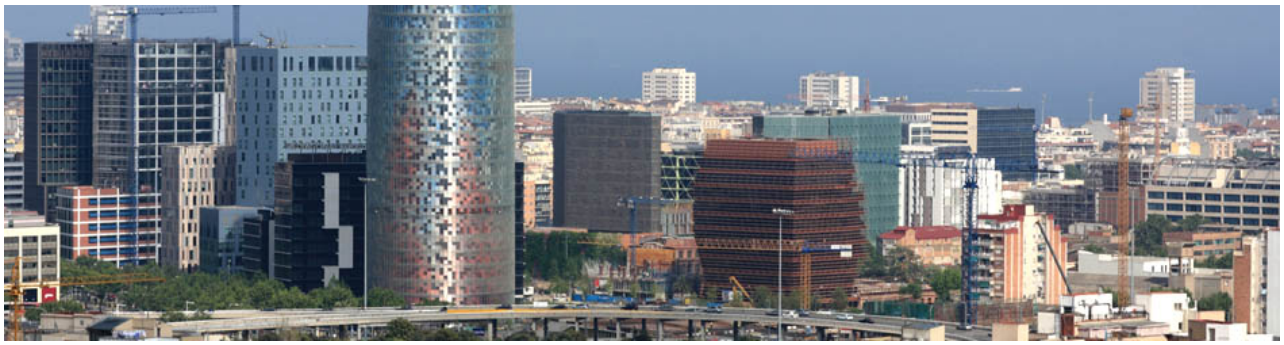
Michael Kim
Senior Foreign Attorney
Kim & Chang
T +82-2-3703-1732
michael.kim@kimchang.com

Ari Yoon
senior Korean Attorney
Kim and Chang
T +82 2 3703 4568
ari.yoon@kimchang.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SPAIN



Last modified 22 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

After a long delay the Spanish Parliament approved the new Spanish Fundamental Law on Data Protection and digital rights guarantee developing and refining the GDPR in December 2018. It has been in force from 7 December 2018 **(“NLOPD”).**

DEFINITIONS

"Personal data" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4 of the GDPR). A low bar is set for "identifiable" – if the natural person can be identified using *“all means reasonably likely to be used”* (Recital 26 of the GDPR) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

NLOPD is extremely restrictive regarding the processing of criminal convictions and offences data, that shall be forbidden except in very exceptional circumstances. Spain deviates itself notably in this regard from the standard position in the EU, where this prohibition is not usually so strict.

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

Despite following GDPR’s approach in this regard, NLOPD does also regulate certain features related to personal data of deceased people.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities. The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of **"lead supervisory authority"**. Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Spanish competent national supervisory authority is the *Agencia Española de Protección de Datos* (“ **AEPD**”), which also represents Spain on the European Data Protection Board. Regional Data Protection Commissioners do exist to supervise personal data processing by regional public authorities and other entities controlled by regional public authorities.

Contact details of the AEPD

Address

C/Jorge Juan, 6
28001 Madrid
Spain

Telephone

+34 901 100 099 /
+34 91 266 35 17

Website

www.aepd.es

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities. The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

NLOPD requires to do so, even for voluntarily appointed DPOs within a short period of time (10 days).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely.

The NLOPD includes a lengthy list of organisations and companies that are required to appoint a DPO. Accordingly, insurance or reinsurance companies, financial credit institutions, educational institutions, electric and natural gas distributors, and advertising and marketing companies, among others, are required to appoint a DPO. The NLOPD also allows organisations and companies to voluntarily appoint a DPO. Please note that, in either case, the appointment of the DPO must also be communicated to the AEPD using the AEPD online facilities.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organisations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or

- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Indeed, NLOPD has done so in a very intense manner. In 2023, the Spanish AEPD confirmed a new and stricter approach regarding the use of biometric data for monitoring access to offices / workplaces, that should be allowed for the future only in very exceptional circumstances.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

The NLOPD has confirmed this prohibition in very strict terms, with only very extraordinary exceptions (e.g. activities of lawyers and court representatives acting on behalf of their clients, verification imposed by AML law, verification imposed by child-protection law).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data – i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors

that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose;
- the context in which the data have been collected;
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible);
- the possible consequences of the new processing for the data subjects; and
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xls / .xlsx).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorised by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Data protection principles

The NLOPD foresees certain scenarios where the controller shall not be responsible for inaccurate data (provided it has taken all reasonable measures to ensure deletion or rectification without delay).

Criminal Convictions and Offences data

Article 10 of the NLOPD allows lawyers and procedural representatives to process the information provided by their clients related to criminal convictions and offences for the purposes of rendering the corresponding legal services. There are also other isolated exceptions if and when endorsed by the law (e.g. verification imposed by AML law, verification imposed by child protection law).

Processing of administrative offence or penalties

The processing of personal data related to administrative offences or penalties is permitted if it is carried out by the relevant public bodies having sanctioning powers over such offenses, and only to the extent necessary for achieving their legitimate purposes. If those requirements are not met, the processing shall be allowed by an specific law, or be based on the data subject’s consent.

Please note that lawyers and procedural representatives are also allowed to process the information provided by their clients related to administrative offenses or penalties for the purposes of rendering the corresponding legal services.

Credit Solvency Databases

The NLOPD sets out stringent requirements for including personal data on credit solvency databases. In this regard, the information to be provided to data subjects as well as the particularities of the debt are, among others, key aspects to be taken into account.

CCTV Processing

Under the NLOPD, the processing of images through CCTV is only permitted for security purposes, provided that (i) the data obtained is duly deleted within the corresponding period of time (unless it is relevant for evidence purposes), and (ii) the mandatory notice requirements are met. Additional detailed requirements do apply.

Whistleblowing

The processing of personal data relating to whistleblowing (including anonymous reporting) is permitted provided that (i) employees are duly informed ,(ii) whistleblowing databases are only accessed by the necessary persons to carry out internal control purposes or to initiate the relevant disciplinary proceedings, and (iii) the data obtained is duly deleted within the mandatory period of time. Additional detailed requirements do apply.

Unfair competition

The NLOPD generates a new catalogue of “unfair competition practices” linked to personal data.

Data processing for electoral purposes

Political parties, coalitions and electoral groups can use personal data obtained from websites and other public sources to carry out political activities during an election period. Likewise, sending electoral propaganda by electronic means, as well as contracting any such propaganda on social or similar networks will not be deemed a commercial activity.

Transparency (Privacy Notices)

The NLOPD allows (Article11) provision of the information required by Articles 13 and 14 of the GDPR in layers. In this sense, a first layer should include the “basic information” of the relevant processing as well as an immediate and easily accessible form (i.e. a link) to the second layer, where the rest of information to be provided under Articles 13 and 14 of the GDPR shall be included. Please note that the content of the before-mentioned “basic information” depends on each case, but most of the times includes (i) the identity of the controller, (ii) the purpose of the processing, and (iii) the rights under Article 15 – 22 of the GDPR.

Rights of the data subject

Under the NLOPD, a data subject’s right of access is deemed granted when the controller provides him/her with a means that permanently guarantees remote, direct and secure access to his / her personal data. In addition, the NLOPD indicates that more than one right of access request within six months shall be considered repetitive for the purposes of Article 12(5) of the GDPR unless the relevant requests are based on a legitimate reason.

Under the NLOPD, controllers must clearly indicate in their internal information systems the cases where the processing of personal data is restricted.

Blocking right / Blocking duty (NLOPD)

The NLOPD states that following the exercise of rectification or erasure, controllers shall "block" the personal data so that it shall remain available to the relevant public authorities in very specific situations. The NLOPD also offers other alternatives in case the “blocking” of personal data is not feasible or involves a disproportionate effort.

Rights of the deceased

The NLOPD recognizes the right to digital testament. Moreover, the heirs of the deceased are entitled to exercise the rights of access, erasure and rectification of data unless the deceased person would had prohibited it (or if it is not in line with applicable law).

Special category data

The NLOPD deviates from GDPR mainstream approach on special category data. Most of this type of data cannot be processed relying on the consent of the data subject (health, biometric and genetic data being the exception to this ban, but relying on consent may be also not permitted for the latter and even standard data in employment and other contexts).

Location data

The overall position in Spain is that it may be acceptable provided that:

- users are informed at all times on whether the location system is active and retain full control on the system, freely deciding when to switch it on or off;
- the purposes of the processing are legitimate and proportionate and do not harm in an unfair manner the constitutional rights of the data subjects;
- users have been clearly informed on the circumstances under which they can be located and the purposes of such processing;
- users have the option (especially when being off-duty if the location data is used in an employment context) to turn off the system; and
- if in an employment context, Works Council / representatives of the employees, have been informed in advance about the collection of this type of information and the purposes of the processing (which shall remain within the limits of the authority of the employer to direct, control and monitor workers’ professional activities)

One of the main originalities of the NLOPD when compared with the GDPR is that it accepts new “digital rights”, including, i.e. Internet neutrality, universal access to Internet, security of online communications, digital education, protection of minors on the Internet, amendment / update of non-accurate information on the Internet, a right to be forgotten-like right not to be found by search engines on the Internet and social networks.

On top of this, certain provisions of the NLOPD may have an impact on the relationship between a company and its employees (i.e. monitoring of digital devices, digital disconnection of the employees outside working hours, privacy at the workplace).

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). As of 29th November 2022, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, the Eastern Republic of Uruguay, New Zealand, the Republic of Korea (South Korea) and the United Kingdom.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules or EU/AEPD standard contractual clauses (a new version of which was approved by the EU Commission in June 2021). The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities (which remains under NLOPD, however, when EU/AEPD standard contractual clauses are replaced by other sets of clauses or other safeguards).

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4). No minimum threshold, in terms of individuals concerned or financial impact of the breach is set by GDPR or NLOPD regarding the notification obligations.

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

NLOPD has established different levels of infringements (very serious, serious and minor) which are linked to different limitations’ periods (3, 2 and 1 year respectively).

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, since the AEPD defends the viewpoint that e-Marketing laws are more specific than GDPR/NLOPD and shall prevail on the latter when data protection and e-marketing elements do concur (a problem that would not be present when marketing deliverables are provided off electronic channels, in which case other legal bases for processing, like the legitimate interest of the sponsor could be considered again). Where consent is relied upon, AEPD claims that the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is expected to be replaced very soon by a EU-level Regulation, whose drafting procedures are nearly finalised. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive shall be replaced, the AEPD claims, with the GDPR standard for consent.

Electronic Marketing is regulated in Spain specifically by the Spanish Act on the Information Society Services and e-Commerce 34 /2002 ('LSSI'). The general principle is that deliveries of electronic marketing materials are lawful only if they have been explicitly authorised in advance by the recipients (authorisation that is required not just for individuals, but also where the recipient is a legal entity, broadening here the scope of Spanish Data Protection Act). An exception to this general principle applies to deliveries to clients when the materials refer to products/services that are equal or similar to the ones sold to them in the past by the company sponsoring the advertisement.

Electronic publicity shall:

a. be clearly marked as such by means of the terms PUBLI or PUBLICIDAD placed inside the subject line,
b. allow the recipient to opt-out at all times, even at the time of registration, and
c. clearly identify the sponsor of the delivery. It is the sponsor of the delivery, not the electronic publicity company that shall be held liable in case of enforcement. Opt-out shall include an email address when the publicity was delivered by email too. Opt-out procedure shall be simple and free for the recipient of the publicity.

Enforcement shall include, *inter alia*, fines that, in most cases, shall be between EUR 30,000 and EUR 150,000.

The NLOPD states that databases containing the identification details of those data subjects who have expressed their opposition to receiving commercial communications may be created (the so-called “**Robinson’s Lists**”). These databases must be reviewed by the entities sending commercial communications (the access details to these databases will be published by the AEPD) unless the relevant data subjects have previously granted their consent to receiving such commercial communications.

Finally, it shall also be taken into account that that the NLOPD permits processing activities where the purpose is to avoid sending commercial communications to those data subjects who have expressed their opposition to receiving them.

ONLINE PRIVACY

Cookies are regulated in Spain, in addition to the Spanish Data Protection Act, by the Spanish Act on the Information Society Services and e-Commerce (“**LSSI**”), as amended in March 2012. In July 2023, the AEPD released new Guidance Notes on the use of cookies (granting a sunrise period until 11th January 2024 for the data controllers and data processors to implement the new criteria). Although the Guidance Notes are not legally binding they give useful indications on the best market practice and on the criteria that the AEPD would follow when enforcing the law.

The Guidance Notes require data controllers to inform cookies’ recipients – including legal entities – of the existence and use of cookies, their scope and how to deactivate them. The regulator stresses the need for cookies’ sponsors to make sure (and be able to demonstrate later on) that the user has noticed the invitation to install and use the cookies and has voluntarily and unmistakably decided to accept it. Certain types of cookies (e.g. session cookies) are exempt from these restrictions.

KEY CONTACTS

Diego Ramos
Partner
T +349 17901658
diego.ramos@dlapiper.com

Paula González de Castejón
Partner
T +34 91 788 7374
paula.gonzalez@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SRI LANKA

Last modified 3 January 2024

LAW

Sri Lanka until recently did not have legislation pertaining to protection of data and privacy, although different sector specific laws such as the Computer Crimes Act No. 24 of 2007, the Banking Act No. 30 of 1988, the Electronic Transactions Act No. 19 of 2006, the Right to Information Act No. 12 of 2016 and the Telecommunications Act No. 25 of 1991 recognize the need for privacy and confidentiality. Identifying this lacuna, the Personal Data Protection Bill was first published as a draft bill in 2019. It was subject to several rounds of revisions, and subsequently was passed by the Parliament of Sri Lanka on 19 March, 2022 as the Personal Data Act No. 9 of 2022 (“PDPA”).

Although certified by the Speaker of Parliament, except for Part V of the PDPA which deals with provisions relating to the regulator under the law, i.e. the Data Protection Authority, the PDPA is yet to become operative as it provides for different time periods within which certain parts of the law would come into force, allowing controllers and processors a much-needed grace period. The majority of the law will come into operation within 18 to 36 months from the 19 March, 2022, while the part governing the sending of marketing messages using personal data would become operative within 24 to 48 months from the 19 March, 2022. With regard to Part V, it should be noted that an order has been issued by the Minister of Technology which provides that the said Part V of the PDPA has been brought into operation on 17 July, 2023. Accordingly, the Data Protection Authority is now in the process of being established, upon the completion of which the other parts of the PDPA are expected to follow suit.

The PDPA is primarily inspired by the European Union's General Data Protection Regulation (“GDPR”) and, therefore, shares many similarities with the GDPR.

The PDPA applies both territorially to the processing of personal data where such processing takes place wholly or partly within Sri Lanka, or by a person or entity within Sri Lanka; and extraterritorially, in so far as a person or entity outside Sri Lanka provides goods or services to individuals within Sri Lanka or monitors the behaviour of individuals within Sri Lanka.

Whilst the PDPA is the primary law that governs the protection of personal data in Sri Lanka, the following regulations / directions, which have been promulgated under the relevant sector specific laws, contain detailed provisions on data protection which are as follows:

i. The Financial Consumer Protection Regulations No. 1 of 2023 (the “FCPR”), published on the 9 August, 2023, promulgated under the Monetary Law Act, No.58 of 1949 (now replaced by the Central Bank of Sri Lanka Act, No. 16 of 2023), provides obligations substantially similar to the PDPA in relation to the protection of personal information of financial consumers. The FCPR is applicable to licensed commercial banks, licensed specialised banks, licensed finance companies, specialized leasing companies, authorized primary dealers, authorized money brokers, licensed microfinance companies, participants of the payment and settlement systems or any other financial institutions approved by the Central Bank of Sri Lanka. The FCPR provides protection not only to personally identifiable information but also extends to all information pertaining to financial consumers, which includes corporate entities and other legal bodies. The FCPR also provides for grace periods before the same becomes operational, with a majority of the regulations becoming operational

upon the expiration of 6 months from the date of its publication. Additionally, the requirements of the FCPR pertaining to the security of personal information are buttressed by the Regulatory Framework on Technology Risk Management and Resilience for Licensed Banks, directions No. 16 of 2021, dated 9 December 2021, promulgated under the Banking Act No. 30 of 1988 (as amended). The applicability of this framework however is limited to licensed commercial banks and licensed specialized banks in Sri Lanka and its concentration lies on the information security requirements of such organizations.

ii. The Special Direction No. 91 published by the Consumer Affairs Authority on the 17 May, 2023, under the Consumer Affairs Authority Act No. 09 of 2003 (as amended), sets out provisions governing e-commerce entities and platform operators for the purpose of protecting consumers. These directions, although not in extensive detail, enumerate the principles set out in PDPA, aiming to the protect the personal data of consumers. It should be noted that unlike the PDPA, these directions are operational as at date.

DEFINITIONS

Many definitions in the PDPA are similar to that of the GDPR. In particular:

“**Personal data**” is defined to mean any information by which a data subject may be identified, either directly or indirectly by referring to an identifier or one or more factors specific to that individual. Thus, a name of a person is not a necessity for data to constitute personal data, but any factor such as an identification number, financial data, location data or an online identifier or factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that individual that allows for the tracing of him / her, would constitute personal data under the PDPA.

The PDPA further identifies a category of personal data as “special categories of personal data” with a view of protecting more sensitive personal data which are at a higher risk of adversely affecting an individual in the event such data is exploited. Special categories of personal data are defined to include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data and biometric data, data concerning health or a natural person’s sex life or sexual orientation, personal data in relation to offences, criminal proceedings and convictions or personal data relating to a child.

The term ‘processing’ has been rendered an extremely wide meaning within the PDPA to include (but not be limited to) collection, storage, preservation, alteration, retrieval, disclosure, transmission, making available, erasure, destruction of, consultation, alignment, combination, or the carrying out of logical or arithmetical operations on, personal data.

The PDPA places extensive obligations on controllers of personal data. A ‘controller’ is defined to include any natural or legal person / entity which determines the purposes and means of processing personal data. When two or more controllers jointly determine the ways and means of processing personal data, the PDPA identifies them as joint controllers.

A ‘processor’ on the other hand is any natural or legal person / entity which processes personal data on behalf of the controller.

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Authority of Sri Lanka ("**Authority**") is recognized as the regulator of personal data governed by the PDPA. The law provides for comprehensive objects and powers of the Authority as the regulator, which include making rules, issuing guidelines, receiving complaints, conducting inquiries, examining persons under oath, issuing directives and imposing fines in the event of non-compliance with the law.

REGISTRATION

At present, the PDPA does not require registration. Nevertheless, upon the PDPA becoming operative, rules requiring registration may be introduced as the PDPA empowers the Authority to make regulations specifying the categories and criteria of licenses to be issued under the PDPA.

Although not a registration requirement, the PDPA requires controllers and processors to publish the contact details of their data protection officers and ensure that it is communicated to the Authority.

DATA PROTECTION OFFICERS

The PDPA requires controllers and processors which are not public authorities to appoint a Data Protection Officer (“ **DPO**”) where their core activities consist of:

a. processing operations that require regular and systematic monitoring of data subjects on a prescribed scale or magnitude;
b. processing special categories of personal data on a prescribed scale or magnitude; or
c. processing which results in a risk of harm to the rights of the data subjects protected under the PDPA.

The PDPA permits a group of entities to appoint a single DPO provided, however, such DPO is easily accessible by all of the group entities.

Such DPO is required to be a competent individual possessing academic and professional qualifications in matters relating to data protection.

The specific responsibilities of the DPO as per the PDPA includes:

- advising controllers or processers on data processing requirements;
- ensuring on behalf of the controller or processor that the requirements of the PDPA are met;
- enabling capacity building of staff engaging in data processing operations;
- advice on personal data protection impact assessments; and
- co-operation and compliance with all directives and instructions issued by the Authority.

COLLECTION & PROCESSING

Similar to the GDPR, the PDPA enshrines certain principles governing the collection and processing of personal data. Each controller must ensure that personal data is processed in compliance with such principles, which are as follows.

- process lawfully;
- process for specified, explicit and legitimate purposes and not further process in a manner that is incompatible with those purposes;
- process personal data which is adequate, relevant and limited to the purpose;
- ensure that personal data is accurate and where necessary kept up to date;
- keep personal data in a form which permits identification of data subjects for no longer than is necessary, for the purpose (s) for which the data are processed;
- process in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures;
- process in a transparent manner, providing information on such processing to data subjects; and
- ensure accountability in processing by the implementation of internal controls and procedures that are able to demonstrate compliance with the PDPA, identified as the “Data Protection Management Programme”.

Legal Basis

In order to ensure that processing is ‘lawful’ whenever personal data is processed, such processing should be based on the most appropriate legal basis out of the following grounds provided under the PDPA:

- consent of the data subject (consent should be freely given, specific, informed and unambiguous indication in writing or by affirmative action and capable of being withdrawn at any time);
- necessary for the performance of a contract with the data subject in order to take steps at the request of a data subject to enter into a contract with such data subject;
- necessary for compliance with a legal obligation to which the controller / processor is subject to under Sri Lanka law;
- necessary to respond to an emergency that threatens the life, health or safety of the data subject or another natural person;
- necessary for the performance of a task carried out in the public interest or in the exercise of powers, functions or duties imposed under Sri Lanka law; or

- necessary for the purposes of legitimate interests of the controller or a third party (subject to an assessment where the interests of the controller should be balanced against the rights of the data subjects and accordingly, must not override the interests of the data subject, especially when the data subject is a child).

Special Categories of Personal Data

In addition to the aforesaid lawful grounds, if processing special categories of personal data, a controller is required to satisfy one of the following additional conditions, on the objective basis of being most appropriate:

- consent of the data subject, which in the case of a child will mean the consent of the parent or legal guardian;
- processing is necessary for the purposes of carrying out the obligations of the controller and exercising of the rights of the data subject, in the field of employment, social security including pension and for public health purposes in so far as it is provided for in Sri Lanka Law, providing for appropriate safeguards for rights of the data subject;
- processing is necessary to respond to an emergency that threatens the life, health or safety of the data subject or another natural person who is incapable of giving consent;
- relates to personal data which is manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims;
- processing is necessary for any purpose as provided for under any written law in Sri Lanka or public interest;
- processing is necessary for medical purposes and where such data is processed by a health professional licensed under or authorized by any written law in Sri Lanka; or
- processing is necessary for archiving purposes in the public interest, scientific, historical research or statistical purposes in accordance with law.

Criminal Investigations

The PDPA provides for the processing of personal data in relation to criminal investigations, only where such processing is carried out in accordance with written laws in Sri Lanka, whilst providing for appropriate safeguards for the rights and freedoms of data subjects, which may be prescribed in the future upon the PDPA becoming operative.

Transparency of Data Processing

Transparency is an important principle enshrined in the PDPA and, as stated above, it aims to ensure that data subjects are aware of how their personal data is processed and understand their rights pertaining to such data.

Accordingly, the PDPA requires controllers to provide detailed information to data subjects in a concise, transparent, intelligible and easily accessible form. Therefore, providing the following information to data subjects at the point of collection of their personal data is imperative, which can be fulfilled by the provision of a privacy notice:

- identity and contact details of the controller;
- contact details of the data protection officer (where there is a DPO);
- intended purpose for collecting personal data and the legal basis for the processing;
- legitimate interest pursued by the controller (where applicable);
- categories of personal data collected;
- right of data subjects to withdraw consent for processing and method of withdrawing such consent (if processing is based on consent);
- recipients and third parties with whom personal data will be shared;
- details of cross border data transfer;
- period of data retention;
- rights of data subjects with regard to their personal data and how such rights may be exercised;
- right to file a complaint with the Data Protection Authority (“**Authority**”);
- whether the provision of personal data is a statutory or contractual requirement and the consequences of failing to provide such personal data;
- the existence of automated individual decision-making including profiling and the consequences for the data subject.

In addition, when a controller intends to process personal data for a new purpose, a data subject must be informed of such further processing, providing them with the information set out above.

If in any event personal data is collected via means other than direct collection from the data subject, the above information should be provided to the data subject within one month or at the time of the first communication to that data subject or when the personal data is first disclosed to another recipient, whichever event occurs first.

Rights of Data Subjects

The PDPA provides a series of rights for data subjects, largely similar to that of the GDPR. A controller must respond to any written request made by a data subject pertaining to his rights within 21 working days of receiving the request.

Right to access personal data: data subjects have the right to access their personal data, be provided with confirmation as to whether such personal data has been processed and be provided a copy of such personal data by submitting a written request.

Right to withdraw consent: if processing is based on consent, the data subject has the right to withdraw such consent at any time and the right to request a controller to refrain from further processing of the data subject’s personal data, provided the processing was based on the data subject’s consent.

Right to object to processing: data subjects have the right to object to further processing beyond the original purpose for which it was collected where such processing is based on the grounds of legitimate interests or public interest.

Right to rectification or completion: data subjects have the right to request a controller to rectify or complete any personal data that is inaccurate or incomplete.

Right to request a review of automated decisions: a data subject has the right to request for a review of a decision made by a controller based solely on automated processing which is likely to create “an irreversible and continuous impact on the rights and freedoms of the data subject” under Sri Lankan law, unless such automated processing is:

- authorized by Sri Lanka law;
- authorized in a manner determined by the Authority;
- based on the data subject’s consent; or
- necessary for entering into a performance of a contract between the data subject and the controller.

Right to erasure: the data subject may, under a limited set of circumstances, request the controller to erase their personal data. This includes when a controller is in contravention of its obligations and when the erasure is mandated by a written law of Sri Lanka or order of a competent court.

A controller is permitted to refuse to a request of a data subject based on the above rights only in limited instances, having regard to the following:

- national security;
- public order;
- any inquiry, investigation or procedure carried out under Sri Lanka law;
- the prevention, investigation and prosecution of criminal offences;
- the execution of criminal penalties;
- the protection of the rights and fundamental freedoms of persons under Sri Lanka law;
- where the controller is unable to establish the identity of a data subject;
- the requirement to process personal data under any other law in Sri Lanka.

TRANSFER

The PDPA allows for cross-border data flow and the processing of data in a third country outside Sri Lanka, subject to the parameters set out in the PDPA.

In case of a public authority acting as a controller or a processor, such transfer should only be made to a third country prescribed pursuant to an adequacy decision. The Minister in charge of the subject matter has the power to make an adequacy decision in consultation with the Authority, and factors such as the relevant written laws and the enforcement mechanisms available in such third country will be considered in making such an adequacy decision.

A controller or processer that is not a public authority may also process personal data in a third country subject to an adequacy decision. If no adequacy decision has been made, personal data may be transferred to such third country only where the controller or processor effecting such transfer is able to ensure compliance with the obligations imposed under Part I, II and sections 20 to 25 of the PDPA by the imposition of appropriate safeguards. The transferor effecting such transfer is required to adopt an instrument that may be specified by the Authority in order to ensure compliance with the provisions of the PDPA by the transferee.

It is noteworthy that no such adequacy decisions have been made yet, considering the fact that the majority of the law is yet to become operative.

In the absence of an adequacy decision or appropriate safeguards, the PDPA provides the following limited instances where personal data could still be transferred to a third country (provided that the transferor in such instance is not a public authority):

- the data subject has explicitly consented, upon having been informed of the risks of such processing;
- the transfer is necessary for the performance of a contract between the data subject and the controller, or the implementation of any pre-contractual measures taken by the controller at the request of the data subject;
- the transfer is necessary for the establishment, exercise or defence of legal claims relating to the data subject;
- the transfer is necessary for reasons of public interest;
- the transfer is necessary to respond to an emergency that threatens the life, health, or safety of the data subject or another person and where the data subject is incapable of giving consent; or
- any other condition that may be prescribed under the PDPA in the future.

SECURITY

The PDPA does not prescribe the specific technical measures or standards that ought to be implemented but requires the adoption of appropriate technical and organizational measures to ensure security that is commensurate to the risk of the processing activity.

Nonetheless, it provides insight into such technical and organizational measures by setting out that such measures include encryption, pseudonymization, anonymization or access controls.

Moreover, the PDPA also requires processors of personal data to have in place such technical and organizational measures, and ensure that their personnel data are bound by contractual obligations of confidentiality and secrecy.

BREACH NOTIFICATION

A ‘personal data breach’ is broadly defined in the PDPA to mean “*any act or omission that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed*”. The PDPA imposes a general obligation on a controller to notify the Authority in the event of a personal data breach.

The manner, form and the time period within which such notification should be made is to be prescribed by way of rules made under the PDPA, which are likely to be published upon the Authority being established. Accordingly, the threshold for a notifiable breach, the timeframe within which such notification has to be made, and the circumstances where the Authority and the data subjects should be notified, are yet to be specified under the PDPA.

Additionally, the Data Protection Management programme, which is required to be implemented by every controller, must also include a mechanism to detect breaches of personal data.

ENFORCEMENT

Enforcement of the PDPA is carried out by the Data Protection Authority of Sri Lanka (“**Authority**”). As an initial step, the PDPA provides that data subjects aggrieved by the decisions of controllers have the right appeal to the Authority. The Authority is empowered to conduct investigations, and to allow or disallow such appeals at its discretion. In the event an appeal is allowed, the controller in question is required to give effect to the decision of the Authority, and inform the action taken in line with such decision, to both the relevant data subject and the Authority.

The Authority is also empowered to conduct inquiries on a complaint made, or otherwise if the Authority believes that a controller or a processor *inter alia* has contravened, is acting in contravention of or is likely to contravene the PDPA or any other legislation in Sri Lanka relating to processing of personal data.

The Authority has wide powers in conducting inquiries, which includes requiring persons to appear before it, examine persons under oath or affirmation and require the furnishing of information relating to the processing functions of a controller or processor.

Corrective Powers

Upon an inquiry where the controller or processor will be given an opportunity to be heard, the Authority is empowered to issue a binding directive which may include any one or more of the following:

- cease and refrain from the activity in question;
- take certain measured to rectify the situation;
- pay compensation to the person aggrieved.

Administrative Penalties

In the event a controller or processor fails to comply with directives issued by the Authority, the Authority may impose a penalty that will not exceed LKR ten million (10,000,000) for each non-compliance.

In imposing a penalty, the Authority will consider a number of factors, including the following:

- the nature, gravity and duration of the contravention;
- action taken by the controller or processor to mitigate the damage suffered by data subjects;
- the effectiveness of the controller’s data protection management programme;
- the degree of co-operation by the controller with the Authority, in remedying the contravention and mitigating any adverse effects;
- the categories of personal data affected by the contravention;
- whether the controller or processor notified the Authority of the contravention;
- previous contraventions by controller or processor;
- financial benefits gained or losses avoided by the contravention.

Where a controller or processor has been subject to a penalty on a previous occasion and subsequently does not conform to a directive by the Authority, in addition to the penalty, such controller or processor will be liable to pay an additional penalty of twice the amount imposed as the penalty.

If the payment of a penalty is in default, the Authority may make an *ex-parte* application to the Magistrate Court of Colombo for an order requiring the payment, which can be recovered as a fine imposed by such court, even if such fine exceeds the amount such courts in its ordinary jurisdiction would impose.

The PDPA however makes provisions for an appeal to the Court of Appeal to a controller or processor that is aggrieved by the imposition of a penalty, which appeal should be referred within 21 working days from the date the notice of the imposition of such penalty was communicated to such controller or processor.

ELECTRONIC MARKETING

The data protection principles enshrined in the PDPA apply in relation to any electronic marketing activity carried out using personal data.

In addition, if direct marketing messages are to be sent using electronic or any other means, the controller must first obtain consent from the data subject prior to sending such message, which are identified as ‘**solicited messages**’ under the law.

Therefore, unlike the GDPR, legitimate interests cannot be used as the legal basis for processing personal data in sending electronic marketing messages to data subjects.

Consent under the PDPA is required to be freely given, specific, informed and unambiguous indication in writing or by affirmative action. The conditions governing consent under the PDPA set out that:

- the controller should be able to demonstrate that consent was obtained from the data subject;
- if consent is provided in a written form which also concerns other matters, the request for consent should be clearly distinguishable;
- the performance of a contract should not be conditional on a data subject’s consent to processing his personal data that is not necessary for the same; and
- the data subject must be informed, before they give consent, that they may withdraw consent at any time.

Additionally, when sending solicited messages, the controller should:

- provide the data subject information on how they may opt out of receiving such messages, free of charge; and
- inform the data subject of the nature of the message, to whom it is intended, and the identity of the controller or the third party on whose behalf the controller is disseminating the message.

The PDPA also allows the Authority to introduce rules, codes or prefixes that controllers should adopt to identify different categories of solicited messages. However, given that the law is in its transitional stage, such rules have not yet been introduced.

The aforesaid restrictions on marketing would not apply where marketing is aimed at corporate subscribers.

ONLINE PRIVACY

At present there are no requirements specifically applicable to aspects of online privacy such as cookies and location data. However, controllers and processors would be required to adhere to the general obligations set out in the PDPA, and data subjects would still be eligible to the rights and protections afforded to their personal data under the PDPA, when personal data is processed for online purposes.

KEY CONTACTS

FJ&G de Saram
www.fjgdesaram.com/

Shanaka Gunasekara
Partner
T +94 74 390 2018
shanaka.gunasekara@fjgdesaram.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SWEDEN

Last modified 22 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organisation is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organsation that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

In addition to the GDPR, the Data Protection Act (2018:218) (the "**Data Protection Act**") and the Data Protection Ordinance (2018:219) apply. The Data Protection Act regulates general aspects of data protection where the GDPR allows, e.g. processing of personal identity numbers and processing of data relating to criminal convictions and offences. The Data Protection Act applies from 25 May 2018 (i.e. the same date as the GDPR).

In addition to the Data Protection Act and the Data Protection Ordinance, there are sector and processing specific regulations.

The Camera Surveillance Act (2018:1200) contains provisions regarding camera surveillance. The Camera Surveillance Act applies inter alia where camera surveillance is carried out with equipment located in Sweden and where the one carrying out the surveillance is established in Sweden or in a third country. The Camera Surveillance Act applies from 25 May 2018 (i.e. the same date as the GDPR).

The Whistleblowing Act (2021:890) entered into force on 17 December 2022 and implements the EU Directive 2019 /1937 (the Whistleblowing Directive). Chapter 7 of the Whistleblowing Act contains *inter alia* provisions on permitted purposes of processing personal data, internal access to personal data and retention periods.

Moreover, a vast number of sector specific acts apply in Sweden, for example relating to the healthcare, ethical review of research, finance, education, referendums / elections, enterprise, communication, certain aspects of the labor market, etc.

For example, the Credit Information Act (1973:1173) applies to credit reference agencies and contains specific provisions regarding the processing of personal data.

The Patient Data Act (2008:355) and the Patient Data Ordinance (2008:360) regulates healthcare providers' processing of personal data. As of 1 January 2023, the new the Act (2022:913) on shared health and care documentation applies. It contains further provisions regarding the processing of personal data.

Furthermore the Electronic Communications Act (2022:482) (the "**Electronic Communications Act**") and the Electronic Communications Ordinance (2022:511) apply to inter alia electronic communications networks and electronic communications services and associated facilities and services as well as other radio use. The Electronic Communications Act implements Directive (EU) 2018/1972 (the Electronic Communications Code) and Directive 2002/58/EC (the so called ePrivacy Directive). The Electronic Communications Act applies to providers of public electronic communications networks and publicly available electronic communications services' processing of personal data, and regulates the use of so-called cookies.

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the Cnil in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

In Sweden, the Swedish Authority for Privacy Protection (Sw: Integritetsskyddsmyndigheten) is the supervisory authority.

Postal address

Box 8114
104 20 Stockholm
Sweden

Visiting address

Fleminggatan 14, 7th Floor
112 26 Stockholm
Sweden

Phone number

+46 8 657 61 00

E-mail

imy@imy.se

Website

www.imy.se

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases (Article 36 prior consultation) following a data protection impact assessment (Article 35) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

In Swedish national law, there are no indiscriminate general notification obligations. However, there are sector and processing specific provisions requiring notification and / or requiring a permit from the relevant supervisory authority, *inter alia*:

- A permit from the Swedish Authority for Privacy Protection is required for camera surveillance of publicly accessible areas carried out by authorities (and under limited circumstances private entities tasked with similar duties as authorities) under the Camera Surveillance Act (2018:1200).
- With a limited number of exceptions, the processing of personal data relating to criminal convictions and offences (Article 10 of the GDPR) by others than public authorities requires a permit from the Swedish Authority for Privacy Protection under the Data Protection Act and the Data Protection Ordinance (2018:219). The Swedish Authority For Privacy Protection has proposed a new regulation to allow for companies in the financial sector and in the defence industry to process personal data relating to criminal convictions and offences.
- Sector specific requirements exist under *inter alia* the Credit Information Act (1973:1173). A license from the supervisory authority is generally required to carry out credit information activities. From 1 January 2024, the responsibility for issuing licences and supervising credit information activities will be transferred from the Swedish Authority for Privacy Protection to the Swedish Financial Supervisory Authority (Sw: *Finansinspektionen*).

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must report directly to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

There are no derogations in Swedish national law, except that under the Data Protection Act, a DPO performing tasks under to Article 37 GDPR shall not unauthorisedly disclose what has come to their knowledge in the performance of their tasks. The Swedish Public Access to Information and Secrecy Act (2009:400) applies in relation to the confidentiality obligation of a DPO within the public sector.

COLLECTION & PROCESSING

Data protection principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimisation principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organisational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organisations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal basis under article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special category data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;

- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal convictions and offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorised by Member State domestic law (Article 10).

Processing for a secondary purpose

Increasingly, organisations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose;
- the context in which the data have been collected;
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible);
- the possible consequences of the new processing for the data subjects; and
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (privacy notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;

- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the data subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorised by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

Personal identity numbers

In Sweden, personal identity numbers may be processed without consent only where manifestly justified with regard to the purpose of the processing, the importance of secure identification or some other substantial reason.

Personal data relating to criminal convictions and offences

Personal data relating to criminal convictions and offences (Article 10 of the GDPR) may be processed by other parties than public authorities if the processing is necessary to (i) establish, exercise or defend legal claims or (ii) to fulfil a legal obligation under law or regulation. Furthermore, the Swedish Authority for Privacy Protection may upon application in an individual case grant a permit to process personal data relating to criminal convictions and offences.

Rights of the data subject

Swedish law may prohibit controllers to disclose certain data to data subjects. This applies to the rights in Articles 13-15 of the GDPR.

For personal data in running text which has not taken on its final form when the request was made (e.g. drafts) or that is a note or similar, the right under Article 15 of the GDPR does not apply. This exemption may however not be relied on by a data controller if such personal data (i) has been disclosed to a third party, (ii) is processed solely for archiving purposes in the public interest or for statistical purposes, or (iii) has been processed over a period of more than one year in running text that has not taken on its final form.

Other derogations for specific processing situations or sectors

Furthermore, in regards to data subjects' rights, there are a number of sector specific derogations (e.g. healthcare and credit reference agencies, etc.).

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). On 10 July 2023, the European Commission adopted its adequacy decision for the EU-US Data Privacy Framework, in which an adequate level of protection for personal data transferred from the EU to US companies that have joined the framework

is ensured in accordance with GDPR Art. 45. Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, Republic of Korea, Eastern Republic of Uruguay, the United Kingdom, United States (if certified under the EU-US Data Privacy Framework) and New Zealand.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules and standard contractual clauses. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

On 16 July 2020, the Court of Justice of the European Union's ("**CJEU**") invalidated the EU-US Privacy Shield in the so called Screms II case (judgement of the CJEU in Case C-311/18). Moreover, the CJEU clarified that exporters of personal data to third countries may continue to rely on standard contractual clauses. When doing so, however, exporters need to carry out a so-called transfer impact assessment and implement supplementary measures as necessary in each individual case, in order to be able to ensure that a level of protection essentially equivalent to that which is guaranteed within the EU can be upheld.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

- explicit informed consent has been obtained;
- the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
- the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation. Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

There are no specific security requirements set out in the Data Protection Act. However, it should be noted that certain security related provisions are prescribed under the Patient Data Act (2008:355) when processing personal data, regarding e.g. confidentiality, access and disclosure.

Moreover, a two-factor authentication when accessing special categories of data over an open network and encryption when sending special categories of data are examples of previous recommendations from the Swedish Authority for Privacy Protection.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

There are no derogations under Swedish law, except that personal data breaches that fall under the Criminal Data Act (2018:1177) (which implements the Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data) shall be reported by public authorities separately in accordance certain provisions of the Criminal Data Act.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

Fines

Under the Data Protection Act, infringements of Article 10 of the GDPR may render administrative fines. As regards the amount of such fines, the higher of the two levels for legal maximum fines prescribed in the GDPR applies (Article 83(5) of the GDPR). As such, fines may be up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher.

In relation to public authorities, violations of the GDPR may render administrative fines under the Data Protection Act. Fines imposed on public authorities adhere to the system of the two levels of fines depending on the violated Article set out in the GDPR, may amount to maximum SEK 5 000 000 (in relation to the lower level of fines, set out in Article 83(4) of the GDPR) and SEK 10 000 000 (in relation to violations set out in Articles 83(5) and 83(6) of the GDPR).

Moreover, the Data Protection Act regulates procedural matters relating to decisions on administrative fines and how to appeal such decisions made by authorities (for example, the right to appeal to the Swedish Administrative Court).

Right to damages

The right for data subjects to claim damages from a controller or processor under Article 82 of the GDPR also applies to violations of provisions in the Data Protection Act and other Swedish regulations that supplement the GDPR.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (“ePrivacy Directive”), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

There is no provision in the Data Protection Act which particularly concerns the processing of personal data in relation to electronic marketing.

There is, however, other legislation in Sweden (such as the Marketing Act (2008:486) that regulates electronic marketing in Sweden.

Under the Marketing Act, unsolicited automated electronic marketing (by *inter alia* email) to natural persons generally requires prior consent. It is, however, allowed to conduct email marketing to natural persons without prior consent provided that the person has not objected to such, if the trader has received the email address of the individual in

connection with sales of a similar product. In these cases, the addressee must be given the option to opt out of marketing both when the email address is collected and subsequently along with each marketing email.

The Marketing Act also states that, in the case of email marketing, the email message must always contain a valid address to which the recipient can send a request for the marketing to cease. This applies to marketing to natural persons as well as to legal entities.

Note that certain provisions relating to electronic marketing under Swedish law may be amended in the future due to the upcoming ePrivacy Regulation which will become immediately enforceable as law in all EU member states.

ONLINE PRIVACY

Pursuant to the Electronic Communications Act (implementing *inter alia* the e-Privacy Directive), data may be stored in or retrieved from a subscriber's or a user’s terminal equipment only if the subscriber or user has been provided with information about the purpose of the processing and consents to it, i.e. the user must give its prior ‘opt-in’ consent before a cookie is placed on the user’s computer. In its judgment of 1 October 2019, the Court of Justice of the European Union (the "**CJEU**") decided on cookie consent requirements and stated that cookie consent must be given by a statement or clear affirmative action (consent cannot be validly obtained through pre-ticked checkboxes).

Consent is however not required for storage or access that is:

- necessary for the transmission of an electronic message over an electronic communications network; or
- necessary for the provision of a service explicitly requested by the user or subscriber.

In the event of a wilful or negligent breach of the now relevant provision in the Electronic Communications Act are criminalised. As such, a fine may be imposed provided that the offence is not sanctioned by the Swedish Criminal Code (1962:700). However, if the breach is deemed to be minor, no fine shall be imposed. To our knowledge there has not yet been any cases where a website operator has been fined for a breach of the cookie provision in the Electronic Communications Act.

Sweden has set the digital age of consent as 13 in relation to consent to processing of personal data in the context of offering information society services.

KEY CONTACTS

Jennie Nilsson
Advokat / Partner, Head of Digital, Data & Cyber
T +46 73 867 67 87
jennie.nilsson@se.dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

SWITZERLAND

Last modified 22 August 2023

LAW

The processing of personal data is mainly regulated by the Federal Act on Data Protection of 25 September 2020 (FADP) and its ordinances, i.e., the Ordinance on Data Protection (ODP) and the Ordinance on Data Protection Certification. The FADP (including its ordinances) has entered into force on 1 September 2023 and become effective without any transition period.

The FADP has recently been revised with the aim to strengthen data protection in general and to align it with the requirements of the EU General Data Protection Regulation (GDPR) in order to facilitate compliance of Swiss companies with those aspects of the GDPR that are applicable to controllers or processors outside of the EU, and to ensure that the EU will continue to consider Switzerland as providing an adequate level of data protection. However, the FADP continues to provide for certain deviations from the GDPR, thus requiring certain “Swiss Add-Ons” in a number of areas.

The processing of personal data is further restricted by provisions in other laws, mainly with regard to the public sector and regulated markets.

Key differences between the former and the new FADP

- Scope of “personal data”: The former FADP was applicable to personal data pertaining to both natural persons and legal persons. In contrast, the new FADP only protects personal data of natural persons.
- Data processing principles: While the data processing principles have essentially remained the same, the new FADP, in addition, explicitly provides for the principles of “privacy by design” and “privacy by default”.
- Information obligation: With the new FADP, an extended duty to inform data subjects has been introduced.
- Additional obligations: The new FADP imposes a number of additional obligations. In particular, the controller and /or processor must, under certain circumstances, maintain records of processing activities, perform data protection impact assessments and notify data security breaches.
- Data subject rights: With the new FADP, certain data subject rights have been extended and a new right to data portability has been introduced.
- Supervisory authority: The new FADP grants the supervisory authority expanded powers, in particular to issue administrative measures in the event that data protection provisions have been violated.

Sanctions: While the new FADP continues to provide for criminal sanctions that are (primarily) directed against the responsible individual, the catalogue of punishable offences has been extended and the fines have been significantly increased.

Territorial scope

The FADP, like the GDPR, has an extraterritorial scope and is applicable to circumstances that have an effect in Switzerland, even if they were initiated abroad. This includes, for instance, international companies with group entities in Switzerland or, under certain circumstances, international companies even without such subsidiary in Switzerland based on their doing business in Switzerland. For civil claims, the Swiss conflict of law rules apply.

In addition, the FADP provides that private controllers domiciled abroad must designate a representative in Switzerland if they process personal data of data subjects in Switzerland and if the data processing fulfils all of the following requirements:

- The processing is connected to offering goods or services in Switzerland or to monitoring the behaviour of data subjects in Switzerland;
- the processing is extensive;
- the processing is carried out regularly;
- the processing involves a high risk for the personality of the data subjects.

DEFINITIONS

Definition of personal data

Personal data means any information relating to an identified or identifiable natural person. In contrast to its previous version, the FADP does no longer apply to personal data pertaining to legal persons.

Definition of sensitive personal data

Sensitive personal data is defined as:

- Data relating to religious, philosophical, political or trade union-related views or activities;
- data relating to health, the intimate sphere or the affiliation to a race or ethnicity;
- genetic data;
- biometric data that uniquely identifies a natural person;
- data relating to administrative and criminal proceedings or sanctions;
- data relating to social assistance measures.

Profiling and high-risk profiling

Profiling means any form of automated processing of personal data consisting of the use of such data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

High-risk profiling means profiling that poses a high risk to the data subject's personality or fundamental rights by matching data that allow an assessment to be made of essential aspects of the personality of a natural person.

High-risk profiling is subject to certain stricter requirements.

Breach of data security

Breach of data security means a breach of security that leads to the accidental or unlawful loss, deletion, destruction or modification or unauthorised disclosure of or access to personal data.

NATIONAL DATA PROTECTION AUTHORITY

Federal Data Protection and Information Commissioner (FDPIC)
Feldeggweg 1
CH - 3003 Berne Switzerland
T +41 (0)58 462 43 95
F +41 (0)58 465 99 96

Website and contact forms: https://www.edoeb.admin.ch/

The FDPIC supervises and advises federal and private bodies, comments on federal legislative projects and informs the public about his findings and rulings in cases of general interests.

REGISTRATION

The FADP does not require the registration of any data collections or processing activities for private data controllers. Instead, the FADP provides for a general duty for controllers and processors to maintain a record of processing activities (ROPA). The controller's ROPA shall at least contain the following information:

- The controller's identity;
- the purpose of the processing;
- a description of the categories of data subjects and the categories of processed personal data;
- the categories of the recipients;
- if possible, the period of storage of the personal data or the criteria to determine this period;
- if possible, a general description of the measures taken to guarantee data security;
- if the data is disclosed abroad, details of the country concerned and the implemented guarantees.

The processor's ROPA may be limited to information on the identity of the processor and of the controller, the categories of processing activities performed on behalf of the controller as well as, if possible, a general description of the data security measures and, in case of cross-border data transfer, the details of the country concerned and the implemented guarantees.

However, companies with less than 250 employees as well as natural persons do not have to maintain a ROPA unless:

- They process sensitive personal data on a large scale; or
- they carry out high-risk profiling.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer (DPO).

However, controllers have the option to appoint a DPO as a contact point for the data subjects and the competent data protection authorities. A DPO's main tasks would be to train and advise private controllers in data protection matters and to participate in the implementation of data protection regulations.

The controller may also designate an “independent” DPO who meets certain additional qualifications. In such a case, the controller has to ensure that the DPO has all necessary resources (including access to the data processing activities and personal data) to fulfil its tasks and has the right to inform the management or governing body regarding important data protection matters. Additionally, the DPO must exercise its function in a professionally independent manner and without being bound by instructions from the controller and shall not perform any activities which are incompatible with its tasks as DPO. The DPO shall also possess the required expertise. Finally, the contact details of the DPO must be published and notified to the FDPIC.

In case an “independent” DPO is appointed, the controller has no obligation to consult with the FDPIC in the event that a data protection impact assessment indicates a high risk to the personality or the fundamental rights of the data subject despite the planned measures by the controller (see here). This is the only relief granted in case of appointing an “ independent” DPO.

COLLECTION & PROCESSING

Data Processing Principles and Duties

The following principles apply to the collection and processing of personal data:

- Personal data may only be processed lawfully, in good faith and in accordance with the principle of proportionality.

- The collection of personal data and, in particular, the purpose of its processing must be evident to the data subject. In addition, the FADP imposes the following duties on controllers:
    - a duty to inform the data subject about the collection of personal data similar as under the GDPR, with the list of minimum information being shorter, but drafted more openly and in a non-exhaustive manner (however, the FADP goes beyond the GDPR in that it requires the controller to specify all countries to which personal data is transferred, or from which it is accessed, and to provide some additional information in this context);
    - under certain circumstances a duty to inform the data subject about decisions based solely on automated processing that have legal consequences or significant impact on the data subject (automated individual decision).

Wilful violations of the information duty may be subject to sanctions (see here).

- Personal data should only be processed for a purpose that is indicated or agreed at the time of collection, evident from the circumstances at the time of collection, and/or provided for by law.
- The controller and any processor must ensure that the data processed is accurate.
- Personal data must not be transferred abroad if the privacy of the data subject may be seriously endangered (see here).
- The controller must design the processing in technical and organisational terms to comply with data protection law, in particular the (other) data processing principles (privacy by design). Furthermore, the controller is obliged to ensure by means of suitable default settings that the processing is limited to the minimum required for the respective purpose (privacy by default).
- Personal data must be protected from unlawful and unauthorized processing by appropriate technical and organisational measures.
- Personal data must not be processed against the explicit will of the data subject, unless this is justified by:
    - an overriding private or public interest; or
- Sensitive personal data must not be disclosed to a third party, unless this is justified by:
    - the consent of the data subject (which must be given expressly in addition to being voluntary and based on adequate information);
    - an overriding private or public interest; or
- Personal data shall be destroyed or anonymized as soon as it is no longer required for the respective processing purpose.

The FADP imposes on the controller a duty to conduct a data protection impact assessment if the processing may constitute a high risk for the personality or the fundamental rights of the data subject (particularly when new technologies are used) and also defines specific cases where a data protection impact assessment may be necessary, including in the event of processing sensitive personal data on a large scale and systematic surveillance of extensive public areas. The FDPIC generally needs to be consulted if the data protection impact assessment shows that the processing presents a high risk for the personality or fundamental rights of the data subject despite the measures envisaged by the controller.

Rights of the Data Subject

Data subjects enjoy certain rights to control the processing of their personal data:

Right of access

A data subject is generally entitled to request access to, and obtain a copy of, his or her personal data that is being processed (i.e. the personal data as such), together with prescribed information on the identity and contact details of the controller, the purpose of processing, as well as the period of storage of the personal data (or the criteria used to determine the period) and the available information about the source of the personal data, if it has not been collected from the data subject. If applicable, the data subject is also entitled to be informed about the existence of an automated individual decision and the logic on which this decision is based as well as the recipients (or categories of recipients) to which the personal data is disclosed. In case of cross-border data transfer, the destination country and the implemented guarantee (if applicable) shall also be provided to the data subject. There are certain exceptions, e.g. a data controller may invoke its own overriding interests, however, only if it does not disclose the personal data to third parties (whereby companies controlled by the same legal entity are not considered third parties).

Wilful violations of data subject access rights by giving incomplete or wrong information are subject to sanctions (see here).

Right to rectify / Right to erasure / Right to restriction of processing / Right to object

The data subject may request that inaccurate personal data concerning him or her be corrected. Taking into account the purpose of the processing, he or she may also request that incomplete personal data be completed. This right is, however, restricted to the extent that a legal provision prohibits the modification or the personal data is processed for archival purposes in the public interest.

If the personal data is processed unlawfully and there is no justification (i.e. consent, overriding private or public interest or legal basis), the personal data must be deleted or destroyed. Under such circumstances, the data subjects may also request that the data processing be prohibited or restricted or they may object to the processing in question.

Right to data portability

Data subjects may request the controller to deliver the personal data that they have disclosed to it in a conventional electronic format if the controller is carrying out automated processing of the data and if the personal data is being processed with the consent of the data subject or in direct connection with the conclusion or the performance of a contract between the controller and the data subject. In addition, the data subject may request the controller to transfer the personal data to another controller if the aforementioned requirements are met and no disproportionate effort is required. There are certain exceptions, e.g. a data controller may invoke its own overriding interests, however, only if it does not disclose the personal data to third parties.

TRANSFER

Personal data may be transferred outside Switzerland if the destination country offers an adequate level of data protection. The Federal Council maintains and publishes a list of such countries as Annex 1 to the ODP. It should be noted that, under Swiss data protection law, remote access to data residing in Switzerland from outside of Switzerland is also considered a transfer/disclosure abroad.

The Federal Council deems, *inter alia*, the data protection legislations of all EEA countries as well as of the United Kingdom to be adequate. However, the countries covered by an adequacy decision of the European Commission do not fully correspond to those considered as adequate by the Federal Council.

In the absence of legislation that guarantees adequate protection, personal data pertaining to individuals may be disclosed abroad only if at least one of the following conditions is fulfilled:

- Data protection clauses in an agreement between the controller or the processor and its contractual partner that ensure an adequate level of data protection. The use of such clauses must be notified to the FDPIC beforehand.
- Specific guarantees drawn up by the competent federal body that ensure an adequate level of data protection. The use of such guarantees must be notified to the FDPIC beforehand.
- Standard data protection clauses that the FDPIC has approved, issued or recognised beforehand. On 4 June 2021, the European Commission had issued new Standard Contractual Clauses (SCC). According to the FDPIC, these new SCC can also be used to safeguard cross-border data transfers from Switzerland to countries without an adequate level of data protection, provided they are (slightly) amended to comply with the FADP. “Old” safeguards based on the former SCC may no longer be used. Contrary to the former FADP, the FDPIC does not have to be notified about the implementation of SCC anymore. Other safeguards still have to be notified.
- Binding corporate rules that ensure an adequate level of data protection in cross-border data flows within a single legal entity or a group of affiliated companies. Such rules must have been approved by the FDPIC or by the authority responsible for data protection in a country that guarantees an adequate level of protection.
- The data subject explicitly consents to the particular data export.
- The disclosure is directly connected with the conclusion or performance of a contract between the controller and the data subject or between the controller and its contracting partner in the interest of the data subject.
- The disclosure is essential in order to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal rights before a court or another competent foreign authority.
- The disclosure is required in order to protect the life or the physical integrity of the data subject or of a third party and it is not possible to obtain the data subject's consent within a reasonable period of time.

- The data subject has made the personal data generally accessible and has not expressly prohibited its processing.
- The data originates from a register provided for by law which is accessible to the public or to persons with a legitimate interest, provided that the legal conditions for the consultation are met in the specific case.

Violations of certain obligations regarding cross-border transfers of personal data are subject to sanctions (see here).

Regarding cross-border data transfers to the US, the EU and the US have established a new “EU-US Data Privacy Framework” (as successor of the invalidated EU-US Privacy Shield). On 10 July 2023, the EU Commission issued an adequacy decision for the EU-US Data Privacy Framework as the US would ensure an adequate level of protection for personal data transferred from the EU to organisations in the US that are included in the “Data Privacy Framework List”. Therefore, a transfer of personal data from the EU to a US company certified under the EU-US Data Privacy Framework no longer requires additional safeguards pursuant to the GDPR. While neither the EU-US Data Privacy Framework nor the adequacy decision by the EU directly impact data transfers from Switzerland to the US, the FDPIC took, for the time being, note of these developments. It may be anticipated that the Swiss authorities will aim at establishing a similar framework in the foreseeable future.

SECURITY

The data controller and any processor shall guarantee a level of data security appropriate to the risk by taking suitable technical and organisational measures. The measures must make it possible to avoid data security breaches and ensure the confidentiality, availability, integrity and traceability of the personal data. In particular, personal data must be protected against the following risks:

- Unlawful or accidental loss, deletion and destruction;
- technical errors;
- forgery, theft or unlawful use;
- unauthorized altering, copying, accessing or other unauthorized processing.

The technical and organisational measures must be appropriate, in particular with regard to the type of processed data and the purpose, nature, extent and circumstances of the data processing, the risks for the personality or fundamental rights of the data subjects and the current technological standards and implementation costs. The ODP sets out these requirements in more detail.

Wilful violations of the minimum data security requirements (which, however, are only defined generally in the ODP) are subject to sanctions (see here).

BREACH NOTIFICATION

The FADP provides for three different notification obligations in the event a data security breach occurs:

1. The controller shall notify the FDPIC as soon as possible of any data security breach that is likely to lead to a high risk to the data subject's personality or fundamental rights. The FDPIC has made available a reporting portal (see here), which may be used to submit a notification.
2. The controller shall inform the affected data subjects of any data security breach if this is required for their protection or if the FDPIC so requests. Even though the FADP does not stipulate a specific time frame in this regard, it is evident that such information must be provided in a timely manner in order to achieve its purpose.
3. The processor shall notify the controller of any data security breach as soon as possible. The FADP does not provide for a threshold in this respect. Therefore, a notification is required regardless of the specific risk involved.

A data security breach is defined as a breach of security that leads to the accidental or unlawful loss, deletion, destruction or modification or unauthorised disclosure or access to personal data. The ODP details what information a breach notification must contain and imposes a documentation obligation on the controller.

ENFORCEMENT

Investigations by the FDPIC

The FDPIC may initiate an investigation against a federal body or a private person if there are sufficient indications that a data processing activity could violate data protection regulations. If the data protection regulations have been violated, the FDPIC may issue administrative measures, for instance, the FDPIC may order the modification/suspension/termination of the processing and deletion of personal data or delay or even prohibit the disclosure abroad.

Criminal Sanctions

The FADP provides for criminal liability and fines of up to CHF 250,000, which are primarily directed against the responsible natural person (and not the respective company as under the GDPR). In particular, the following duties are subject to criminal fines in the event of certain wilful violations:

- Duty to provide information when collecting personal data and in the case of an automated individual decision;
- duty to provide information upon a data subject access request;
- duty to cooperate with the FDPIC in the context of an investigation;
- duty to meet certain requirements in connection with cross-border data transfers;
- duty to meet certain requirements in connection with the assignment of processors;
- duty to meet certain minimum requirements for data security;
- professional duty of confidentiality;
- duty to comply with a ruling issued by the FDPIC or a decision of the appeal courts.

Criminal proceedings must be initiated by the competent cantonal prosecution authority.

Finally, under Swiss civil law the data subject may apply for injunctive relief and may file a claim for damages as well as satisfaction and/or surrender of profits based on the infringement of his/her privacy.

ELECTRONIC MARKETING

Electronic marketing practices must comply with the provisions of the Swiss Federal Act Against Unfair Competition (UCA).

With regard to the sending of unsolicited automated mass advertisement (which, in addition to emails, includes SMS, automated calls and fax messages), the UCA generally requires prior consent by the recipient, i.e., 'opt-in'. As an exception, mass advertisings may be sent without the consent of the recipient:

- If the sender received the contact information in the course of a sale of his/her products or services;
- if the recipient was given the opportunity to refuse the use of his/her contact information upon collection (opt-out); and
- if the mass advertising relates to similar products or services of the sender.

In addition, mass advertising emails must contain the sender’s correct name, address and email contact and must provide for an easy-access and free of charge ‘opt-out’ from receiving future advertisements.

The UCA generally applies to business-to-consumer as well as to business-to-business relationships, i.e., mass advertisements sent to individuals and to corporations are subject to the same rules.

Direct marketing by telephone is not *per se* impermissible in Switzerland as long as it is not done in an aggressive way (e.g., by repeatedly calling the same person). However, the UCA prohibits direct marketing by telephone:

- If the recipient is not listed in the Swiss telephone directory or if the recipient is listed in the Swiss telephone directory, but has indicated that he/she does not wish to receive advertising from persons with whom he/she has no business relationship; or
- if the caller is not calling from a telephone number that (i) is listed in the Swiss telephone directory, (ii) is shown when calling, and (iii) he/she is entitled to use.

In order to enforce the above criteria, the UCA not only sanctions the violation of these principles, but also the use of information that has been obtained in violation thereof (e.g. someone using the information obtained from non-compliant call centres). An intentional violation can be sanctioned with a custodial sentence of up to three years or a monetary penalty.

In addition to the rules of the UCA, the general data protection principles under the DPA also apply with regard to electronic marketing activities, e.g., the collection and maintenance of email addresses or processing of any other personal data.

ONLINE PRIVACY

The processing of personal data in the context of online services is subject to the general rules pertaining to the processing of personal data under the FADP. In addition, certain aspects of online privacy are covered by other regulations, such as the use of cookies which is also subject to the Swiss Telecommunications Act (TCA).

Under the TCA, the use of cookies is considered to be processing of data on external equipment, e.g., another person’s computer. Such processing is only permitted if users are informed about the processing and its purpose as well as about the means to refuse the processing, e.g., by configuring their web browser to reject cookies.

In addition, the general rules under the FADP apply where cookies collect data related to persons who are identified or identifiable, i.e., personal data. In particular, the controller must provide the data subjects with certain information when collecting personal data (for more details on the information obligation see here). In practice, this is often fulfilled by including a section on cookies in the website's privacy policy or implementing a specific cookie policy. In accordance with the principles of privacy by design and privacy by default, the controller shall furthermore only pre-select essential cookies. Non-essential cookies (e.g. analysing cookies) may, depending on the circumstances, only be used with the data subject's consent.

Where the personal data collected through a cookie is:

- Considered sensitive personal data, e.g., data regarding religious, ideological, political views or activities; or
- so comprehensive that it permits an assessment of essential characteristics of the personality of a person (i.e. high-risk profiling)

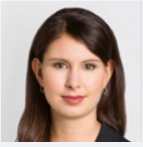
the stricter rules pertaining to the processing of sensitive personal data and high-risk profiling are applicable. These stricter rules provide, *inter alia,* that consent (if necessary) must be given expressly. Furthermore, sensitive personal data may not be disclosed to third parties without justification.

KEY CONTACTS

Schellenberg Wittmer Ltd
www.swlegal.ch/

Roland Mathys
Partner / Attorney at Law
T +41 (0)44 215 3662
roland.mathys@swlegal.ch

Kenzo Thomann
Associate / Attorney at Law
T +41 (0)44 215 3659
kenzo.thomann@swlegal.ch



Helen Reinhart
Associate / Attorney at Law
T +41 (0)44 215 9360
helen.reinhart@swlegal.ch

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

TAIWAN

Last modified 18 December 2023

LAW

The Taiwan Personal Data Protection Act (“**PDPA**”) as most recently amended on May 31, 2023 and the Enforcement Rules of the Personal Data Protection Act (“**Enforcement Rules**”) as most recently amended on March 2, 2016.

DEFINITIONS

Definition of personal data

The PDPA defines “personal data” as the name, date of birth, identification card number, passport number, special traits, fingerprints, marital status, family, education, profession, medical history, medical treatment, genetic information, sexual life (including sexual orientation), health examination, criminal record, contact information, financial condition, and social activities of a natural person, as well as other data by which such person may be directly or indirectly identified.

Definition of sensitive personal data

The PDPA defines “sensitive personal data” as medical records, medical treatment, genetic information, sexual life (including sexual orientation) and health examination and criminal records.

NATIONAL DATA PROTECTION AUTHORITY

Currently, the regulatory body with overall responsibility for data protection is the National Development Council ("**NDC** ”). However, according to the May 31, 2023 amendment of the PDPA, the NDC is expected to be replaced by an independent data protection authority (i.e. the Personal Data Protection Commission). This amendment has not been effective yet and its effective date remains uncertain as of date.

In addition, the authority with jurisdiction over the relevant data collector has primary enforcement responsibility (e.g. the Financial Supervisory Commission has the primary enforcement responsibility *vis-á-vis* financial institutions).

REGISTRATION

Taiwan does not have a registration system for personal data protection.

DATA PROTECTION OFFICERS

The PDPA does not impose a general requirement to have a data protection officer. However, there are industry specific regulations in certain industries (such financial institutions or airlines) requiring personnel to handle personal data protection matters.

COLLECTION & PROCESSING

Under the PDPA, in order to collect, process and use personal data, the data collector is required to give the data subject a privacy notice at the time the data subject’s personal data is first collected. Such privacy notice is required, *inter alia,* to contain:

- the name of the data collector;
- the purpose of collection;
- classification of personal data to be collected;
- time period for the use, geographical area of the use, recipients of the data and the manner of using personal data;
- the rights of the data subject to request to review his / her personal data, to make copies of such personal data, to supplement or correct such personal data, to discontinue collection, processing or use of personal data or to delete such personal data, together with the manner in which the data subject makes such requests; and
- the impact on the data subject’s rights and interests if the data subject chooses not to provide his / her personal data.

As long as the privacy notice is given when the personal data is first collected, and the privacy notice meets the content requirements set out in the PDPA, the privacy notice is by itself considered sufficient (i.e. consent is not required). This is unless sensitive personal data is collected, in which case the data subject’s consent is required.

TRANSFER

The privacy notice to data subjects must set out the extent to which personal data will be transferred to others.

Cross-border transmissions of personal data are regulated by the PDPA. The Taiwan authorities may restrict the cross-border transmission and use of personal data in the following circumstances:

- when a substantial interest of Taiwan is at stake;
- as provided under an international treaty or agreement (as at December 10, 2021, there are no such treaties or agreements in place);
- when the receiving country lacks proper laws or regulations adequately to protect personal data or where infringement of the rights and interests of the data subject is threatened; or
- the purpose of the transfer is to evade the application of the PDPA.

The Taiwan National Communications Commission (NCC) issued an order in 2012 prohibiting communications enterprises from transferring subscribers’ personal data to mainland China; the Ministry of Health and Welfare issued an order in 2022 prohibiting social worker offices from transferring data subjects’ personal data to mainland China; and the Ministry of Labor issued an order in 2023 prohibiting private employment services institutions and employment service agencies for people with disabilities from transferring data subjects’ personal data to mainland China, all on the grounds that the personal data protection laws in mainland China are still inadequate. As at December 18, 2023, there are no other restrictions or prohibitions on the cross-border transfers to any other country / area.

SECURITY

A data collector is required to adopt proper security measures to prevent personal data from being stolen, altered, damaged, destroyed or disclosed.

In addition, the relevant competent authority at the central government level may designate certain data collectors for setting up plans of security measures for personal data files or the disposal measures for personal data after termination of business. As at December 18, 2023, industry specific guidelines governing the plan of security measures for personal data files have been promulgated for many industries, including for financial institutions, human resources recruitment business, hospitals, manufacturers, and others.

BREACH NOTIFICATION

Upon a data breach (which is not defined under the PDPA, however, from a Taiwan law perspective, such would mean where a data subject’s personal data is accessed, taken, revealed, leaked, changed or otherwise infringed on by any unauthorized person or entity or in any unauthorized manner), the data collector is required to promptly notify the data subject of:

- the fact of the infringement;
- the measures the data collector has taken to respond to such infringement; and
- the contact information of the data collector.

No threshold has been provided for when such notice has to be given to the affected data subjects. It is understood that so long as personal data is stolen, disclosed, altered or otherwise infringed on, such notice has to be promptly given.

The notice may be made orally, by written document, telephone, text message, email, facsimile, electronic record, or in another manner which the data subject can receive such notice. If the cost of notifying each data subject is “too high”, such notice may be made via the internet or news media.

In addition, data collectors in certain industries (e.g. travel agents, financial institutions) are required to report to their respective industry regulator and, where it is required to do so, the report to the industry regulator needs to include:

- the fact that personal data may have been compromised;
- the measures the data collector has taken to respond to such compromise (including evidence that the data collector has notified the affected individuals);
- the investigation by the data collector (or any outside forensic firm) as to how the data breach occurred;
- the preventive measure(s) the data collector will take to prevent recurrence of data breach in the future; and
- any other information that the industry regulator may require on a case-by-case basis.

Also, between 2021 and 2023, steps were taken by the Taiwan authorities to expand the material data breach reporting obligations of, *inter alia*, security service providers, pawnshops, travel agents and financial institutions by (i) requiring such enterprises to report material data breaches to the relevant industry competent authority within a specified period (e.g. 72 hours) and / or (ii) requiring such competent authorities to further report such breach to the NDC within 72 hours of becoming aware of the breach. Such steps are now being implemented or will shortly become effective. Also, the term “material data breach”, subject to the relevant regulations, in general means a situation where personal data is stolen, altered, damaged, destroyed or disclosed, and such will endanger the normal business of the data collector, or the rights and interests of a large number of data subjects (“large” has not been defined).

ENFORCEMENT

In addition to civil damages, violations of the PDPA, depending on the specific violation, are also subject to administrative sanctions and criminal sanctions and, in some cases, imprisonment.

Civil damages

If a data collector intentionally or negligently violates any provision of the PDPA and such violation causes illegal collection, processing or use of personal data or other infringement to a data subject, the data collector is liable to compensate the data subject for the damages suffered. Compensation may be both monetary and in the form of corrective measures (e.g. to rectify damage to the data subject’s reputation).

Where the victims may not have access to or cannot provide evidence for the amount of actual damage, the minimum amount is NT$ 500 (approx. US$ 18 as at December 10, 2021) and the maximum is NT$ 20,000 (approx. US$ 690 as at December 10, 2021) per violation / per injured party depending on the severity of the infringement. In the case of class actions, the aggregate total compensation to the class as a whole is limited to NT$ 200,000,000 (approx. US$ 6,900,000 as at December 10, 2021). However, one should not necessarily rely on these limits because the maxima do not apply if it can be proven that a higher amount is appropriate. Furthermore, the limits may be circumvented by resorting to general causes of action in tort over and above the specific statutory cause of action created by the PDPA.

Administrative sanctions

A regulatory body may impose administrative fines on a data collector in violation of the PDPA ranging from NT$ 20,000 (approx. US$ 690 as at December 10, 2021) to NT$ 500,000 (approx. US$ 17,300 as at December 10, 2021) per violation. These administrative fines may be imposed repeatedly until the violation is cured. The May 31, 2023 amendment of the PDPA increases the administrative sanctions on a data collector for its violation of data security obligations to up to NT$15,000,000 (approx. US$ 483,900 as at December 18, 2023), and such increase came into effect on June 2, 2023.

Also, the representative, managers or other persons having authority of the data collector which violates the PDPA are subject to the same administrative fines as the data collector itself, unless it is proven that the relevant representative, manager or other person having authority had properly performed his / her duties. There is no definition of representative, manager or other person having authority but generally such terms are understood to refer to the chairman and the general manager of the company.

Criminal sanctions

A person who, with the intention to gain “benefit” for themself or a third party or to “harm” the interests of others, violates certain requirements as set out in the PDPA or conducts a prohibited cross-border transfer of personal data may be punished by up to five years’ imprisonment and / or fines of up to NT$ 1,000,000 (approx. US$ 35,000 as at December 10, 2021). In addition, the acquisition, dissemination, alteration, compromise of the accuracy of, or deletion of personal data with the intent to gain “benefit” for themself or a third party or to “ harm” the interests of others, in circumstances which is sufficient to cause damage to others, may also be punished by imprisonment for up to five years and / or fines of up to NT$ 1,000,000 (approx. US$ 35,000 as at December 10, 2021).

ELECTRONIC MARKETING

If a data collector wishes to use a data subject’s personal data for the purpose of direct marketing whether electronic or otherwise, such data collector is required to give the data subject a privacy notice (see Collection and Processing).

If a data subject requests the data controller to cease direct marketing, the data collector must stop using the data subject’ s personal data for marketing.

In this regard, when a data collector uses personal data of a data subject to conduct marketing for the first time, the data collector must advise the data subject that they have the right to require cessation of the marketing and provide the data subject with information as to how to exercise such right. Also, the data collector must bear the cost of the first cessation request (e.g. by providing a toll-free line to call or a stamped pre-addressed envelope for return mail).

ONLINE PRIVACY

Although the PDPA does not specifically regulate online privacy, cookies and location data could be considered as social activities of a natural person by which such person may be directly or indirectly identified, as such the PDPA may apply to online privacy.

KEY CONTACTS

Russin & Vecchi
www.rvlaw.ru/taipei

Phoebe Yu
Partner
Russin & Vecchi
T +886-2-2713-6110
pyu@russinvecchi.com.tw

Helen Wang
Associate
Russin & Vecchi

T +886-2-2713-6110
hwang@russinvecchi.com.tw

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

TAJIKISTAN

Last modified 25 November 2022

LAW

- Personal Data Protection Law, No.1537 of 3 August 2018
- Protection Data Law, No.631 of 15 May 2002
- Informatization Law, No. 40 of 6 August 2001 – Legislation has passed (April 04, 2019, No 1595) that amends and supplements the Informatization Law but the amendments are only of a terminological nature.
- Information Law, No.609 of 10 May, 2002
- Regulation on Certification of Information Security Facilities, Attestation of Information Objects and the Procedure for Their State Registration, No.404 of 1 October 2004
- The List of Information Security Facilities Subject to State Certification, No.424 of 24 February 2008
- The decree of the Communication Service under the Government of the Republic of Tajikistan “On the Procedure of implementation by the owner, operator and third party of measures for personal data protection” dated 02.07.2021, #2.21-11

DEFINITIONS

Personal Data Protection Law (hereinafter '**PDPL**') identifies personal data as any information about the facts, events and circumstances of the life of a data subject, which allow to identify him / her.

Under the foregoing law the data subject is considered a physical person, to whom relevant personal data refers.

PDPL does not define the term of sensitive data. However it provides the definition of biometric personal data which includes biometrical and physiological data which identifies the data subject. Biometric personal data may be collected upon receipt of the subject’s consent.

NATIONAL DATA PROTECTION AUTHORITY

The Main Department is Communication Service under the Government of the Republic of Tajikistan (hereafter '**Regulator**').

Address:

57 Rudaki avenue
Dushanbe, Tajikistan
734001

Tel: +992 37 223 11 53
info@khadamotialoqa.tj
Website: khadamotialoqa.tj

REGISTRATION

Under PDPL pre-notification of the Regulator while collecting, processing or maintaining a database consisting of personal data is not required.

However, Data Protection Law requires to certify all information security facilities (including cryptographic, software, organizational, technical and hardware-based), as well as foreign made facilities designated for the protection of information.

The list of information protection facilities is set forth by the Main Department for the Protection of State Secrets under the Government of the Republic of Tajikistan (Regulator). Certification is carried out on the basis of an agreement concluded between Regulator and data controller.

DATA PROTECTION OFFICERS

Tajik law does not require to appoint any Data Protection Officer or any similar positions.

COLLECTION & PROCESSING

PDPL provides the following definitions of collection and processing of personal data:

- Collection of personal data is an action aimed at receiving personal data
- Processing of personal data are actions aimed at:
    - Recording
    - Systemization
    - Storage
    - Amendment
    - Replenishment
    - Extraction
    - Usage
    - Spread
    - Impersonation
    - Blocking, and
    - Destruction of personal data

Collection and processing of personal data is allowed when the following conditions are met:

- The data subject’s consent or that of his / her legal representatives
- The processed and collected information is in compliance with the lawful aims of the data controller
- The processed and collected information is accurate and complete
- The data subject has access to the processed and collected data relating to him / her and has the right to require rectification of the relevant information
- The data collector has duly certified all the relevant equipments and facilities designated for processing and collection of data with the Regulator

Article 11 of the PDPL entitles the data collector to process personal data without receiving the data subject’s consent, if it is necessary for governmental authorities to carry out their functions or for the purpose of protecting the constitution rights and freedom of the citizens.

TRANSFER

Transfer of personal data is allowed if the rights and freedom of the data subject are not violated. With regard to cross-border transfers of personal data the PDPL does not impose any restrictions on the data controller if the foreign country provides adequate protection of personal data.

Where there is no adequate protection of personal data, a cross border transfer is permitted in the following cases:

- The data subject’s consent is obtained
- The transfer is provided pursuant to an international treaty recognized by Tajikistan, or
- The transfer is necessary for the purpose of protecting citizens rights and freedom, health and morality and public order of the state

SECURITY

The data controller is obliged to take appropriate measures against unauthorized processing, accidental loss, or modification of personal data.

BREACH NOTIFICATION

Currently, there is no formal requirement in Tajikistan to report data breaches to any authority or data subject.

ENFORCEMENT

Enforcement of Data Protection Law ('DPL') is primary done by the Main Department for the Protection of State Secrets under the government of Tajikistan.

In addition, Tajikistan courts, the Prosecutor’s Office, the Ministry of Internal Affairs and other law enforcement bodies have the authority to ensure compliance and enforce the provisions of DPL within their competence.

Violations of DPL may result in civil, administrative and criminal sanctions, including:

- Administrative fines up to approximately USD1,700
- Imprisonment of up to 10 years, and
- The right to claim compensation of damages, including emotional distress under civil proceedings

ELECTRONIC MARKETING

Currently, there is no law or regulation in Tajikistan that specifically regulates electronic marketing.

ONLINE PRIVACY

Currently, there is no law or regulation in Tajikistan that specifically regulates online privacy.

KEY CONTACTS

Alisher Hoshimov
Senior Associate
Centil Law Firm
T +992900878833
alisher.k@centil.law

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

TANZANIA

Last modified 25 January 2024

LAW

On 1 May 2023, the Personal Data Protection Act, 2022 (“**PDPA**”) came into force. The PDPA provides for matters relating to protection of personal data and establishes the principles guiding and conditions for collection and processing of personal data. The principles guiding protection of personal data are provided under section 5 of the PDPA, which include:

i. personal data must be processed lawfully, fairly, in a transparent manner ensuring its security and in accordance with the right to privacy of the data subject;
ii. personal data must be collected for explicit, specified, and legitimate purposes and not further processed contrary to those purposes;
iii. personal data must be accurate and kept up to date and corrected or deleted without delay when inaccurate;
iv. personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
v. personal data must be kept in a form which identifies the data subjects for longer than is necessary for the purposes for which it was processed; and
vi. personal data must not be transferred outside Tanzania contrary to the provisions of the DPA.

In addition, the PDPA provides for the following, among other things:

- Part 2 establishes the Personal Data Protection Commission (“**Commission**”) which will be responsible to ensure implementation of the provisions of the Act. The Commission will also be responsible for registration of data processors and data collectors in Tanzania;
- Part 3 provides for registration of the controllers and processors of personal data;
- Part 4 provides for principles relating to collection, use, disclosure and storage of personal data;
- Part 5 provides for transfer of personal data outside Tanzania; and
- Part 6 provides for rights of the data subjects.

The Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023 (“**PDPA Regulations** ”) made under the PDPA also came into effect on 4 July 2023 and make provisions for matters connected with the PDPA.

The PDPA and its Regulations are the principal data protection laws, supplementing other laws providing for data protection in Tanzania, including the Constitution of the United Republic of Tanzania, 1977 (“**Constitution**”) and other sector specific legislations, for instance the Electronic and Postal Communications Act, 2010 (“**EPOCA**”) and its regulations applicable to the electronic and postal communication sector and the National Payment System Act, 2015 (“ **NPS Act**”) and the Bank of Tanzania (Financial Consumer Protection) Regulations, 2019 applicable to the financial services sector.

DEFINITIONS

Definition of Personal Data

The PDPA defines “personal data” as data about an identified or identifiable person that is recorded in any form, including such person’s:

- personal data relating to the race, national or ethnic origin, religion, age or marital status;
- personal data relating to the education, medical history, criminal or employment history;
- identification number, symbol or other assigned particular;
- address, fingerprints, or blood type;
- name appearing in the personal data of another person or where the disclosure of that name itself will reveal the personal data of that person; and
- correspondence sent to a data collector by the data subject that is explicitly or implicitly of a private or confidential nature, and responses to such correspondence that would reveal the personal data about the individual.[1]

Definition of Sensitive Personal Data

The PDPA defines “sensitive personal data” to include the following information:

- genetic data, data related to children, data related to offences, financial transactions of an individual, security measures or biometric data;
- if processed for what they reveal, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, affiliation, trade union membership, gender and data concerning health or sexual life; and
- any personal data which according to the laws of the country is considered to present a major risk to the rights and interests of the data subject.[2]

1: Section 3 of the DPA

2: Ibid

NATIONAL DATA PROTECTION AUTHORITY

The PDPA provides for establishment of the Commission which will be responsible for monitoring and implementation of the provisions of PDPA in Tanzania. The Commission is yet to be established, but its functions are currently handled under the Ministry of Information, Communication, and Information Technology.

REGISTRATION

Every person collecting or processing personal data must be registered with the Commission.[1] Registration is valid for 5 years.[2]

1: Section 14 of the DPA
2: Section 16 of the DPA

DATA PROTECTION OFFICERS

Data controllers or processors must appoint a data protection officer whose role is to ensure that the control and security measures are in place to protect personal data that is collected or processed.[1] The data protection officer must, among other things, also ensure compliance of the PDPA and its regulations in the processing of the personal data by the data controller or processor, handle applications or complaints made by data subjects, their representatives or any other person to the data controller or processor in relation to the collection or processing of personal data and prepare and submit quarterly compliance reports to the Commission.[2]

1: Section 27(3) of the DPA

2: Regulation 32 of the PDPA Regulations

COLLECTION & PROCESSING

The PDPA requires the data controllers to collect personal data directly from the data subject concerned.[1] The exception is where:

- the personal data is already in the public domain;
- the data subject has consented to the collection of his personal data from another person;
- compliance is not reasonably practicable in the current circumstances;
- non-compliance is necessary for compliance with other written laws; or
- compliance would prejudice the lawful purpose for which the collection is sought.

Prior to collecting personal data, the controller must ensure that the data subject is aware:

- of the purpose for which the personal data is being collected;
- of the fact that the collection of personal data is for authorised purposes; and
- any intended recipients of the personal data.[2]

Further, the controller or processor must ensure the data subject understands what they have consented to and must be afforded a simplified means to withdraw their consent.[3]

Personal data collected must only be used for the intended purpose.[4] Where a data controller collects personal data for any particular purpose, he cannot use such data for a different purpose unless:

- the data subject has consented to the use of his personal data for such purpose;
- the use of the data for such purpose is authorised or required by law;
- there is a direct correlation between the purpose for which the personal data is used and that for which the data was collected;
- the information is used in a manner which does not identify the data subject or for statistical or research purposes and is not published in a manner that could reasonably be expected to identify the data subject; and
- the data controller believes on reasonable grounds that the use of such personal data for the other purpose is necessary to prevent or lessen a serious and imminent threat to the health or life of the data subject or another person or to public health or safety; or
- the use of such personal data for that other purpose is necessary for complying with the law.[5]

1: Section 23(1) of the DPA
2: Section 23(2) of the DPA
3: Regulation 25(d) of the PDPA Regulations
4: Section 25(1) of the PDPA
5: Section 25(2) of the PDPA and regulation 26 of the PDPA Regulations

TRANSFER

The PDPA permits the transfer of personal data outside Tanzania only on the following circumstances:

- to a country that has a legal framework that provides for adequate personal data protection (i.e. essentially equivalent levels of protection to that within Tanzania) provided the recipient has established that:

1. such personal data is necessary for the performance of a task carried out in the public interest or pursuant to the lawful functions of a data controller; or
2. the importance of the transfer and there is no reason to assume that the subject's legitimate interests may be prejudiced by the transfer or the processing in the recipient country.[1]

The data controller must carry out a provisional evaluation on the need to transfer such personal data[2] and ensure the recipient of the data only processes the relevant information in the data and for the purpose for which the data was transferred.[3] The recipient of the data must also ensure that the necessity for the transfer of the personal data can be subsequently verified:[4]

- to any other country with appropriate safeguards on the security and protection of personal data provided the data is transferred solely to permit processing authorised to be undertaken by the controller;[5]
- to a country which does not have the adequate level of protection provided the transfer is in accordance with specifications issued by the Minister responsible for Information, Communication and Information Technology, the data subject has consented to such transfer and the transfer is necessary for:
  - the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken at the request of the data subject;
  - conclusion or performance of a contract concluded or to be concluded the controller and another person in the interest of the data subject;
  - or legally required on public interest grounds or the institution, trial defence of a legal claim;
  - protecting the legitimate interests of the data subject; and
  - the transfer is made in accordance with the law and is aimed to provide information to the public and is open for public consultation in general or by anyone who can demonstrate a legitimate interest, to submit their opinion in accordance with a procedure laid down by law.[6]

Prior to the transfer of personal data outside Tanzania, the data controller or processor must apply for and obtain a permit from the Commission.[7] The application is made using a prescribed form which must be accompanied with proof that:

- the recipient country has ratified an international agreement providing requirements for the protection of personal data;
- there is an agreement between Tanzania and the recipient country regarding the protection of personal data; or
- there is a contractual agreement between the person requesting the personal data and the recipient of the personal data who is outside Tanzania.[8]

1: Section 31(2) of the DPA
2: Section 31(3) of the DPA
3: Section 31(5) of the DPA
4: Section 31(4) of the PDPA
5: Section 32(1) of the PDPA
6: Section 32(4) of the PDPA
7: Regulation 20(1) of the PDPA Regulations
8: Regulation 20(3) of the PDPA Regulations.

SECURITY

The PDPA requires data controllers and their representatives to safeguard personal data by taking necessary security measures for the safeguard of such information against any negligent loss or unauthorised destruction, modification, disclosure, access or processing of personal data.[1]

The security measures that a data collector employs must ensure the required level of security by taking into account the following:

a. the state of technological advancement and the costs of implementing such measures; and
b. the nature of personal data that should be protected and the potential risks to the data subject;[2]

Data controllers are also required to appoint a personal data protection officer (refer to above).[3]

Any processing activity by a data processor must be governed by a contract that will specify the relationship between the processor and the controller in such a way that ensures the data processor will act under the instructions of the data controller and that the data processor will be responsible for ensuring compliance with the security standards provided under the PDPA.[4]

1: Section 27(1) of the DPA
2: Section 27(2)(a) and (b) of the DPA
3: Section 27(3) of the DPA
4: Section 27(4) of the DPA

BREACH NOTIFICATION

Data controllers must promptly notify any personal data security breach to the Commission. The breaches notifiable are any security breaches which affect personal data being processed on behalf of the data controller.[1]

Mandatory breach notification

As advised above, it is mandatory for every data controller to, promptly, notify the Commission of any breach of security that may affect personal data which is being processed on their behalf.

1: Section 27(5) of the DPA

ENFORCEMENT

The Commission established under the PDPA is mandated to ensure the implementation and enforcement of the provisions of the PDPA. The Commission has investigative and corrective powers including to:

- receive, investigate and handle complaints related to alleged contraventions of personal data and privacy of persons; and
- investigate and take necessary steps against anything it considers affects the protection of personal data and infringes privacy of individuals.[1]

The Commission is empowered to issue an enforcement notice on any person if satisfied that that such person has failed to comply with the provisions of the PDPA. Through this notice, the Commission will specify the provision of the Act which have been contravened, the steps which must be taken remedy or eliminate the infringement, the period within which such measures must be implemented (which cannot be less than 21 days), and any right to appeal.[2]

Where the person fails to comply with the enforcement notice and the Commission is satisfied to that effect, the Commission can issue a penalty notice requiring the person to pay fine to be specified in the notice. In determining whether to give a penalty notice and the fine payable, the Commission is required to consider the following:

a. the nature, gravity and duration of the infringement;
b. the intentional or negligent character of the infringement;
c. any measures taken by the data controller or processor to mitigate the damage or distress suffered by data subjects, including technical and administrative / organizational measures;
d. any previous infringements by the data controller or data processor;
e. the degree of co-operation with the Commission, in order to remedy the infringement and mitigate its possible adverse effects;
f. the categories of personal data affected by the infringement;

g. the manner in which the infringement became known to the Commission, including whether the data controller or processor notified the Commissioner of the infringement;
h. the extent to which the data controller or processor had complied with previous enforcement or penalty notices;
i. adherence to approved codes of ethics or terms and conditions of registration;
j. whether a penalty would be effective; and
k. any other aggravating or mitigating factors applicable to the case, including financial benefits gained, or losses suffered, as a result of the infringement (whether directly or indirectly).

The maximum penalty which the Commission may issue in the enforcement notice is Tanzania Shillings One Hundred Million (TZS 100,000,000, approx. US$ 430,000).[3]

The Commission may also direct the controller or processor to pay the affected data subject compensation for infringement of the PDPA and there is no ceiling on the amount of compensation which the Commission can award.[4]

Disclosure of personal data without lawful excuse (including obtaining such data or offering such data for sale) is also a criminal offense which on conviction carries a fine and / or imprisonment. For individuals, the minimum fine for a violation is Tanzania Shillings One Hundred Thousand (TZS 100,000, approx. US$43) and the maximum is Tanzania Shillings Twenty Million (TZS 20,000,000, approx. US$ 8,600).

The maximum term an individual may be sentenced for violating a provision under the PDPA is ten (10) years. If found in violation of the PDPA, an individual may be required to both pay a fine and serve a sentence.[5]

For a company or corporation, the minimum fine for a violation is Tanzania Shillings One Million (TZS 1,000,000, approx. US$ 430) and the maximum is Tanzania Shillings Five Billion (TZS 5,000,000,000, approx. US$ 2,150,000).[6]

1: Section 7(c) and (d) of the DPA
2: Section 45(1) and (2) of the DPA
3: Section 46 and 47 of the DPA
4: Section 50 of the DPA
5: Section 60(6)(a) and Section 61 of the DPA
6: Section 60(6)(b) of the DPA

ELECTRONIC MARKETING

The PDPA refers to regulations to be made relating to commercial use of personal data. It provides that a data subject can enter into a contract with a data controller for the processing of his / her personal data for pecuniary benefits or request a data controller to cease using his / her personal data for direct marketing in accordance with procedures to be set out in regulations to be made under the PDPA.[1]

The PDPA Regulations entitle a data subject to request a data controller or processor to erase or destroy the personal data held by them if the processing of such data is for commercial purposes and the data subject is unwilling for his data to be used commercially.[2] Where processing of personal data is by automated means for the purpose of evaluating matters related to a data subject or is likely to constitute the sole basis for any decision which significantly affects the subject, a data controller must also notify a data subject of the logic involved in that decision and their right to object to the use of their personal data in commercial advertisements.[3]

As advised above, the PDPA requires data controllers and processors to process personal data for the specific purpose for which it has been collected (*Please refer to our advice on Collection Processing of Data above on the requirements to be complied with by the data controllers and data processors while using personal data*). This implies that a person cannot use personal data obtained under the PDPA for commercial use, including electronic marketing, except with the consent from the data subject unless such use is authorised under any written law in Tanzania and the data subject has been informed of such use at the time the data was collected.

Further, financial services providers are prohibited from sharing consumers’ information with a third party for any purpose, including electronic marketing, unless such information is used for the purpose that is consistent with the purpose for which it was originally collected, and the prior written consent of the affected consumer has been obtained before such information is used for any promotional offers.[4]

1: Section 35 of the DPA
2: Regulation 17(d) of the PDPA Regulations
3: Section 33(1)(c) of the PDPA and regulation 19(2)(e) of the PDPA Regulations
4: Regulation 39(b) and (c), Financial Consumer Protection Regulations

ONLINE PRIVACY

Any use of cookies and other third-party trackers which can identify a natural person will qualify as disclosure of personal data and be subject to the PDPA. The PDPA requires data controllers and processors to process personal data for the specific purpose for which it has been collected (*Please refer to our advice on Collection Processing of Data above on the requirements to be complied with by the data collectors and data processors while using personal data*).

This implies that a person cannot use cookies and third-party trackers to process personal data except with the consent from the data subject unless such use is authorised under any written law in Tanzania and the data subject has been informed of such use at the time the data was collected. The data controller must ensure that consent is provided on the basis of information that allows the data subjects to easily identify who the controller is and to understand what they are agreeing to. The controller must also clearly describe the purpose for data processing for which consent is requested.

KEY CONTACTS

DLA Piper Africa, IMMMA Advocates
www.dlapiperafrica.co.tz/en/tanzania/

Madina Chenge
Partner
DLA Piper Africa, IMMMA Advocates
T +255 22 2211080/1/2/3
Madina.Chenge@immma.dlapiperafrica.co.tz

Miriam Bachuba
Senior Associate
DLA Piper Africa, IMMMA Advocates
T +255 22 2211080/1/2/3
Miriam.Bachuba@immma.dlapiperafrica.co.tz

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

THAILAND

Last modified 5 January 2024

LAW

On 28 May 2019, the Personal Data Protection Act ("**PDPA**") became law in Thailand. There was an original one–year grace period for the formation of the Personal Data Protection Committee and the issuance of subordinate regulations, as well as for organisations to become compliant with the PDPA. However, on 21 May 2020, the Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020) ("**Royal Decree**") was published in the Royal Gazette, which effectively extended the implementation of the key provisions of the PDPA until 31 May 2021. On 8 May 2021, an amendment to the Royal Decree was published in the Royal Gazette (Royal Decree No. 2), which postpone the full enforcement of the PDPA for another year. The PDPA then came into full force on 1 June 2022.

In January 2022, the Personal Data Protection Committee was established. Various public hearings on the subordinate regulations have been held. A few of these subordinate regulations have been published, while some are undergoing a public hearing process.

Key principles under the PDPA are highly influenced by the EU General Data Protection Regulation (often referred to as GDPR) regime, but with some key local differences. The PDPA acknowledges individual data subjects' right to control how their personal data is collected, stored, processed, and disseminated by data controllers, provides lawful bases for the processing of personal data, as well as prescribes the duties and responsibilities of data controllers and processors. Whilst Thailand has adapted several concepts from the GDPR, there are still some unique national perspectives in the provisions of privacy notice and data subject rights, notably as regards consent. The data protection obligations under the PDPA generally apply to all organisations that collect, use, or disclose personal data in Thailand or of Thai residents, regardless of whether they are formed or recognised under Thai law, and whether they are residents or have a business presence in Thailand. This extraterritorial scope of the PDPA represents a significant expansion of Thailand's data protection obligations to cover all processing activities relating to Thailand–based data subjects.

Data controllers are permitted to continue to process personal data collected before 1 June 2022 if the purpose for which the personal data was collected remains the same. However, data controllers must publicise a consent withdrawal method and notify the data subjects of the same so that data subjects have the option to withdraw their consent / opt–out. However, if a data controller uses or discloses personal data beyond the original purpose for which the data subjects had previously given consent, further specific consent is required for each separate purpose.

DEFINITIONS

Data Controller is defined as "*a person or juristic person who determines the purposes for which and the manner in which any personal data are, or are to be processed*." Data Controllers have primary responsibility for ensuring that processing activities are compliant with the PDPA.

Data Processor is defined as "*a person or an entity that collects, uses, or discloses personal data on behalf of, or in accordance with, the instructions of a Data Controller*." Data Processors have direct liability under the PDPA in areas such as (this is not exhaustive) data security, data transfer and record keeping.

Personal Data is defined as "*any data pertaining to a person that enables the identification of that person, whether directly or indirectly, but specifically excluding data of the deceased*."

Sensitive Personal Data is defined as "*personal data relating to a person’s race, ethnicity, political opinion, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health, disability, labour union, genetics, biometric or any data which may affect the data subject in the same way as prescribed by the Regulator*." The PDPA requires Sensitive Personal Data to be handled carefully. We expect the Personal Data Protection Committee to provide further guidance on this in due course.

Personal Data Breach is defined as “*a breach of security measures which causes loss, accessibility, usage, alteration, modification, or disclosure of personal data without authorization or unlawfully, whether or not by intention, deliberation, negligence, unauthorized or unlawful acts, a commission of computer offenses, cyber threats, errors or accidents, or any other causes.*”

NATIONAL DATA PROTECTION AUTHORITY

The Personal Data Protection Committee ("**Regulator**") has been established to supervise compliance with the PDPA, under the supervision of the Minister of Digital Economy and Society.

REGISTRATION

The PDPA does not require any registration of Data Controllers, Data Processors or data processing activities. This may change when subordinate laws are enacted.

DATA PROTECTION OFFICERS

Data Controllers and Data Processors are only required to appoint a data protection officer (DPO) if it qualifies as any of the following:

- is a public authority as prescribed and announced by the Regulator;
- requires regular monitoring of Personal Data or system due to the collection, use or disclosure of large amount of Personal Data as prescribed by the Regulator; or
- the core activity of the Data Controller or the Data Processor involves the collection, use, or disclosure of Sensitive Personal Data.

The relevant subordinate regulation was issued on 14 September 2023. It sets out criteria of the core activities of Data Controllers and Data Processors that require ‘regular monitoring’ and indicates factors to be considered in determining a ‘large amount’ of Personal Data. For example, if the core activities consist of tracking, monitoring, analysing, or profiling of personal behaviour or characteristics, and generally involve the processing of Personal Data in a systematic manner and on a regular basis, such core activities require ‘regular monitoring’. If the processing of Personal Data is of 100,000 data subjects or more, or for behavioural advertising purpose via search engine or social media, or by insurance company, financial institution, or licensed telecommunications operator, such processing is considered the processing of ‘large amount’ of Personal Data.

COLLECTION & PROCESSING

Legal bases for collection and processing

The collection, use or disclosure of Personal Data requires consent of the data subject unless other legal bases for processing apply. These include, among other things, the performance of contract or legal obligations, or by legitimate interest of the Data Controller. The legal bases of processing Personal Data and Sensitive Personal Data are different. Due to the sensitive nature of Sensitive Personal Data, explicit consent is required for its collection, use and disclosure without relying on the other legal bases set out in the PDPA (such as vital interest, public health interest and preventive medicine where consent cannot be obtained).

The request for consent must be: (i) explicitly made in writing or via electronic means; (ii) clearly separated from other messages; (iii) delivered in a format which is easily accessible and understandable using language that is easy to understand; and (iv) the message should not be misleading or cause data subjects to misunderstand the purpose of collection. The Data Controller

must also ensure that the consent is freely given and not conditional on entering into a contract. The Regulator can "*require the Data Controllers to request consent from the data subject in accordance with the form and statement prescribed by the Committee*". However, in practice, requiring compliance through a prescribed form may prove challenging, given that Data Controllers may develop their own mechanisms for gaining and assessing consent.

In addition to the above consent requirement, the official guideline on data subject consent issued by the Regulator further prescribed that the consent given by the data subject must indicate a clear affirmative action that the data subject consents to the specific purposes. The examples given under the guideline include data subjects clicking the checkbox, double clicking screen, or screen swiping to affirm their intention to give consent.

Data subjects also have the right to refuse to consent, and the right to withdraw any consent they have given, at any time. Following any such refusal or withdrawal of consent, Data Controllers should be wary of proceeding with the proposed data processing activity.

Notice

Data Controllers must give notice to the data subjects that Personal Data or Sensitive Personal Data is being collected, prior to or at the time of collection, regardless of whether consent or other legal bases of processing apply. The privacy notice must contain particulars prescribed by the PDPA, including categories of persons or entities to whom the collected Personal Data may be disclosed to and the purpose of collection.

The official guideline on privacy notice issued by the Regulator further prescribes that the privacy notice may be given by electronic means, such as a URL link or QR code, and that the language used in a privacy notice should be clear and easily understandable.

TRANSFER

The Data Controller may not use or disclose Personal Data without consent unless it has been exempted from the consent requirement (i.e. on the grounds of other legal bases of processing). The recipient of the Personal Data must not disclose the Personal Data for any other purposes other than as previously notified to the Data Controller when requesting for the Personal Data.

In the event that the Data Controller uses or discloses Personal Data which is exempt from the consent requirement (i.e. other legal basis of processing), the Data Controller must maintain a record of such use or disclosure in the manner prescribed under the PDPA, for example the record must be kept in a written or electronic format.

Processing between Data Controllers and Data Processors

As the Data Processor will be carrying out activities only pursuant to the instructions given by the Data Controller, the PDPA imposes an obligation on the Data Controller to ensure that there is a data processing agreement in place between the Data Controller and Data Processor governing the activities of the Data Processor.

Cross-Border Transfer

Personal Data may not be transferred outside of Thailand, unless the recipient country or international organisation has adequate personal data protection standards in the Regulator’s view and the transfer is in accordance with the rules prescribed by the Regulator. Exemptions may apply such as in the following cases:

- the data subject has given consent and proper notification has been given by the Data Controller;
- the transfer is necessary for the performance of a contract between the Data Controller and data subject; or
- the transfer is necessary in order to protect the vital interests of the data subject.

According to the subordinate regulation regarding the criteria for protecting Personal Data sent or transferred abroad issued on 25 December 2023, the cross-border transfer rules do not apply to the sending and receiving of Personal Data as an intermediary for data transit or data storage that has technical measures to protect unauthorized access from third parties, such as cloud computing services.

As the relevant subordinate regulations have already been issued, the Regulator may soon issue the list of destination or data receiving countries which are considered to have adequate personal data protection standards pursuant to the PDPA.

Transfer between group companies may be exempt from the above requirement if the international transfer is to an organisation within the same group / affiliated business and such transfer is for joint business operations. Nevertheless, the personal data protection policy of such group companies or so called the binding corporate rules (BCR) must be approved by the Regulator. The relevant Data Controller or Data Processor may submit the BCR to the Regulator for approval via post or electronic channel as prescribed by the Regulator.

However, in the absence of a BCR or a decision on the adequate personal data protection standards of the destination country, the Data Controller or Data Processor may transfer Personal Data to another country if it provides appropriate measures as prescribed by the subordinate regulation. Such measures must, for instance, be legally enforceable and binding on all relevant parties, uphold the data subject rights and complaint, and implement the security measures as prescribed by the PDPA.

The subordinate regulation further prescribes that the appropriate measures may be in the form of contract, certification, or provisions in the bill, or binding agreement between Thai and international governmental bodies.

In addition, the subordinate regulation stipulates that the appropriate measure in a form of contract must have either of the following characters:

1. the contract must rely on the international form of contract i.e. ASEAN Model Contractual Clauses for Cross Border Data Flow, Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to the European Union regulation or GDPR, or the standard contractual clauses for sending or transferring of Personal Data of other international organisation as prescribed by the Regulator; or
2. the contract must contain some provisions as prescribed by the Regulator. For example, in case of contract between the Data Controller and Data Controller, the receiving party must inform the transferring party of data breach incident within 72 hours upon becoming aware; or in case of contract between the Data Controller and Data Processor, the receiving party must contact the transferring party if there is any data subject’s right request, and it must delete the Personal Data obtained as requested by the transferring party.

The transfer requirements may have an impact on multinational organisations that routinely transfer data cross border. However, given that many organisations in Europe will already comply with similar (and likely more stringent) data protection laws, the impact of the PDPA may be limited regarding cross–border transfer of data.

SECURITY

Under the PDPA, Data Controllers are required to have appropriate security measures to protect the stored Personal Data against loss, unauthorized and unlawful access, use, alteration, edit or disclosure. Such security measures must be subject to periodic review.

Notification of the Regulator on Security Measures of Data Controller B.E. 2565 (2022), a subordinate regulation under the PDPA, further prescribed that those appropriate security measures shall include organizational measures, technical measures, and physical measures. Examples of security measures include access controls, user access management, user responsibilities, and audit traits.

Data Controllers (and Data Processors) under the PDPA are also now required under the said subordinate regulation to notify staff, employees and / or any relevant persons of the security measures in order to raise awareness of the importance of personal data protection and encourage strict compliance.

BREACH NOTIFICATION

General provisions of the PDPA provide that, in the event of a Personal Data Breach, Data Controllers must report the breach to the Regulator without undue delay, and in any event, if feasible, within 72 hours of becoming aware of it. Data Controllers also have an obligation to notify the data subjects of the breach and the remedial measures if the breach is likely to result in high risks to the rights and freedoms of individuals.

Notification of the Regulator on Rules and Methods of Personal Data Breach Notification B.E. 2565 (2022), a subordinate regulation under the PDPA, prescribed a general procedure upon the Data Controller who is being informed, or becomes aware of actual or potential Personal Data Breach, which includes the following:

- To conduct an initial investigation concerning the Personal Data Breach, to confirm that there is actually a breach and assess the risk that may affect the rights and freedoms of individuals.
- If there is a high risk that the Personal Data Breach may affect the rights and freedoms of individuals, the Data Controller shall take action to prevent, suppress, or rectify in order to stop the breach from causing additional impacts.
- If there is reasonable ground to believe that there was a Personal Data Breach, the Data Controller shall notify the Regulator of the said breach without undue delay, and where feasible, within 72 hours of becoming aware of such breach.
- If Personal Data Breach has a high risk where it may affect the rights and freedoms of individuals, the Data Controller shall notify the affected data subject of the breach, together with the remedial measures taken. Such notification to the data subject shall be given without undue delay.
- Reviewing security measures or taking any other necessary and suitable measures to stop, respond, rectify, or rehabilitate the current situation, and prevent the impacts of a Personal Data Breach of the same nature from arising in the future.

The breach notification given to the Regulator shall be in written or electronic form (or other methods prescribed by the Regulator) and shall include details such as brief information regarding the nature and category of personal data involved in the Personal Data Breach, Data Controller or DPO contact information, information relating to the impacts that may arise, and measures that the Data Controller uses, or will use to prevent, stop, or rectify the Personal Data Breach.

Where the Data Controller fails to notify the Regulator within 72 hours, the Data Controller shall be subjected to an administrative fine (not exceeding THB 3 million). In this regard, the Data Controller may request to be exempted from the liability for the delayed notification of a Personal Data Breach, by clarifying the reasons and the showing that the delay was caused by unavoidable necessities. Such request must be made to the Regulator, not exceeding 15 days of becoming aware of the breach.

Additionally, if the Data Controller views that the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of individuals, the Data Controller may request to be exempted from the breach notification requirement (i.e. to be exempted from notifying the Regulator in accordance with the list of information). In doing so, the Data Controller must provide the Regulator with information, documents, or evidence to support such a request.

ENFORCEMENT

Since the PDPA has fully come into force, there has been approximately 354 cases of complaints and 382 reports of data breach incidents submitted to the Regulator. While 80 administrative orders have been issued, the details of the cases and orders are not publicly available.

There are three types of penalties under the PDPA — civil, criminal and administrative penalties. The amount of penalty will depend on the offence committed. The maximum administrative fine is THB 5,000,000. Punitive damages may also be awarded by the court but this is limited to twice the amount of actual compensation. In the event that the offender is a juristic person, the director, manager or the responsible person may also be criminally liable under the PDPA if the relevant offence(s) resulted from such person's order, action or omission. It is unclear at this early stage what direction the Regulator will take in terms of actual enforcement.

Data Processors who do not comply with their obligations are liable to an administrative fine under the PDPA. There may also be liability under tort law.

Additionally, the Regulator has issued a subordinate regulation under the PDPA, the Notification of the Regulator on the Criteria for Considering the Issuance of Administrative Fine Order by the Expert Committee B.E. 2565 (2022), under which the severity of the violation or failure to comply with the PDPA shall be determined based on the details of the offense (intentional or gross negligence), the size of the Data Controller or Data Processor’s business, the value of damage and severity caused by such wrongdoing, etc. Based on such severity, the expert committee may give notice and order amendment, or impose an administrative fine on the Data Controller or Data Processor.

Exemption from Enforcement of Certain Provisions of the PDPA

The Royal Decree issued on 17 August 2023 exempts certain obligations of Data Controllers under the PDPA in respect of the processing of Personal Data by the listed authorities, such as the National Anti-Corruption Commission, Department of Revenue, Customs Department, Excise Department. However, the exempted Data Controllers must still provide security measures as prescribed by the Regulator to ensure that the exemption does not unreasonably affect the personal data protection principle.

ELECTRONIC MARKETING

Under the PDPA, data subjects have the right to object to direct marketing (whether or not electronic). Therefore, Data Controllers must ensure that there is an opt–out function implemented throughout the entire processing period.

ONLINE PRIVACY

General rules of the PDPA apply to online privacy.

KEY CONTACTS

Samata Masagee
Partner
T +66 2 686 8520
samata.masagee@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

TONGA

Last modified 15 February 2022

LAW

Based on English common law where not addressed by statute.

DEFINITIONS

Definition of Personal Data

None.

Definition of Sensitive Personal Data

None.

NATIONAL DATA PROTECTION AUTHORITY

None.

REGISTRATION

None.

DATA PROTECTION OFFICERS

None.

COLLECTION & PROCESSING

None.

TRANSFER

None.

SECURITY

None.

BREACH NOTIFICATION

None.

ENFORCEMENT

None.

ELECTRONIC MARKETING

None.

ONLINE PRIVACY

None.

KEY CONTACTS

Stephenson Associates
www.stephensonassociates.to/

Dana Stephenson
Principal
Stephenson Associates
info@stephensonassociates.to

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

TRINIDAD AND TOBAGO

Last modified 26 January 2023

LAW

The Data Protection Act, 2011 (DPA) provides for the protection of personal privacy and information processed and collected by public bodies and private organizations.

The DPA was partially enacted on January 6, 2012 by Legal Notice 2 of 2012, and only Part I and sections 7 to 18, 22, 23, 25(1), 26 and 28 of Part II,42(a),(b) of Part III have come into operation, including the processing of personal information under the control of a public body.

No timetable has been set for enacting the remainder of the DPA, and it is possible that there may be changes to the remainder of the legislation before it is proclaimed.

DEFINITIONS

Definition of personal data

Personal information is defined as information about an identifiable individual that is recorded in any form including:

- The name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual
- The address and telephone number of the individual
- Any identifying number, symbol or other particular identifier designed to identify the individual
- Information relating to the individual's race, nationality or ethnic origin, religion, age or marital status
- Information relating to the education or the medical, criminal or employment history of the individual, or information relating to the financial transactions in which the individual has been involved or which refer to the individual
- Correspondence sent to an establishment by the individual
- Information that is explicitly or implicitly of a private or confidential nature, and any replies to such correspondence that would reveal the contents of the original correspondence
- The views and opinions of any other person about the individual
- The fingerprints, DNA, blood type or other biometric characteristics of the individual

Definition of sensitive personal data

Sensitive personal information is defined as personal information on a person's:

- Racial or ethnic origins
- Political affiliations or trade union membership
- Religious beliefs or other beliefs of a similar nature
- Physical or mental health or condition

- Sexual orientation or sexual life
- Criminal or financial record

NATIONAL DATA PROTECTION AUTHORITY

The Office of the Information Commissioner is responsible for the oversight, interpretation and enforcement of the DPA. It has broad authority, including to authorize the collection of personal information about an individual from third parties and to publish guidelines regarding compliance with the Act.

REGISTRATION

There is no registration requirement under the DPA.

DATA PROTECTION OFFICERS

There is no such requirement under the DPA.

COLLECTION & PROCESSING

The knowledge and consent of the individual is required for the collection, use and disclosure of personal information. Collection must be made in accordance with the purpose identified by the organization collecting the personal information.

Sensitive personal information may not be processed except as specifically permitted by law.

The DPA includes provisions that relate specifically to the collection and processing of personal information by public bodies and private enterprises, however, these are not yet in force. Nevertheless, they are presented below.

Public Bodies

Part III of the DPA provides that a public body may collect and process personal data when the following conditions are met: the collection of that information is expressly authorized by law and

- The information is collected for the purpose of law enforcement
- The information relates directly to and is necessary for an operating program or activity of the public body when the collection of personal information is collected directly from the individual:
    - Another method of collection is authorized by the individual, Information Commissioner or law
    - The information is necessary for medical treatment
    - The information is required for determining the suitability of an award
    - The information is collected for judicial proceedings
    - The information is required for the collection of a debt or fine, or
    - It is required for law enforcement purposes
- The individual is informed of the purpose for collecting his / her personal information; the legal authorization for collecting it and contact details of the official or employee of the public body who can answer the individual's questions about the collection

Private Bodies

Part IV of the DPA provides that the collection and processing of personal information by private organizations must be in accordance with certain Codes of Conduct (which are to be determined by the Office of the Information Commissioner in consultation with the private sector) and the General Privacy Principles (which are currently in force).

Sensitive Information

Sensitive personal information may not be processed by public bodies and private organizations without the consent of the individual unless:

- It is necessary for the healthcare of the individual
- The individual has made the information public
- It is for research or statistical analysis
- It is by law enforcement
- It is for the purpose of determining access to social services, or
- As otherwise authorized by law

TRANSFER

Section 6(l) of the DPA provides that personal information may be transferred outside of Trinidad and Tobago only if the laws in the recipient country povide safeguards for the personal information comparable to those provided by Trinidad and Tobago law.

In this regard, the Office of the Information Commissioner is required to publish a list of countries which have comparable safeguards for personal information as provided by this Act in the Gazette and in at least two newspapers in daily circulation in Trinidad and Tobago. Such list has not been published to date.

Sections 72(1) and (2) of the DPA (neither of which are in force as yet) provide that where a mandatory code is developed for private bodies, at a minimum, it must require that personal information under the custody or control of a private organization not be disclosed to a third party without the consent of the individual to whom it relates, subject to certain conditions. Where personal information under the custody and control of an organization is to be disclosed to a party residing in another jurisdiction, the organization must inform the individual to whom the information relates.

Section 6 of the DPA, which is in force, states that all persons who handle, store or process personal information belonging to another person are subject to the following General Privacy Principles:

- An organization shall be responsible for the personal information under its control.
- The purpose for which personal information is collected shall be identified by the organization before or at the time of collection.
- Knowledge and consent of the individual are required for the collection, use or disclosure of personal information.
- Collection of personal information shall be legally undertaken and be limited to what is necessary in accordance with the purpose identified by the organization.
- Personal information shall only be retained for as long as is necessary for the purpose collected and shall not be disclosed for purposes other than the purpose of collection without the prior consent of the individual.
- Personal information shall be accurate, complete and current, as is necessary for the purpose of collection.
- Personal information is to be protected by such appropriate safeguards according to the sensitivity of the information.
- Sensitive personal information is protected from processing except where specifically permitted by written law.
- Organizations are to make available documents regarding their policies and practices related to the management of personal information to individuals, except where otherwise provided by written law.
- Organizations shall, at the request of the individual, disclose all documents relating to the existence, use and disclosure of personal information, such that the individual can challenge the accuracy and completeness of the information, except where otherwise provided by written law.
- The individual has the ability to challenge the organization’s compliance with the above principles and receive timely and appropriate engagement from the organization.
- Personal information which is requested to be disclosed outside of Trinidad and Tobago shall be regulated and comparable safeguards to those under this Act shall exist in the jurisdiction receiving the personal information.

SECURITY

The DPA generally requires that personal information is protected by appropriate safeguards based on the sensitivity of the information. Sensitive personal information may not be processed except where permitted by law.

BREACH NOTIFICATION

There is no provision in the DPA for notifying data subjects or the Information Commissioner of a security breach.

ENFORCEMENT

The Office of the Information Commissioner is responsible for monitoring the administration of this Act to ensure that its purposes are achieved.

The Information Commissioner has several broad powers to conduct audits and investigations of compliance with the DPA.

Part V of the DPA (which is not in force) details the penalties for contraventions of the DPA and also makes further provisions for the enforcement of the DPA.

ELECTRONIC MARKETING

The DPA has no specific provision regarding electronic marketing.

However, Section 58 of the Electronics Transaction Act (not yet in force) requires that anyone performing the following acts shall provide the consumer with a clearly specified and easily activated option to opt out of receiving future communications:

- Sending unsolicited commercial communications through electronic media to consumers in Trinidad and Tobago
- Knowingly using an intermediary or a telecommunications service provider in Trinidad and Tobago to send unsolicited commercial communications
- Sending unsolicited electronic correspondence to consumers while having a place of business in Trinidad and Tobago

ONLINE PRIVACY

The DPA has no specific provision regarding online privacy.

KEY CONTACTS

M. Hamel Smith & Co.
www.trinidadlaw.com/

Jonathan Walker
Partner
T +1 868 821 5500 ext. 5625
jonathan@trinidadlaw.com

Fanta Punch
Partner
T +1 868 299 0981
fanta@trinidadlaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

TUNISIA

Last modified 22 January 2024

LAW

Law n° 2004-63 dated July 27, 2004, on the Protection of Personal Data regulates personal data, but even before that Tunisia was already a pioneer in its region since 2002 in the field of personal data protection. This law was endorsed by the 2022 constitutional embodiment of the protection of privacy, which has placed this protection at the forefront of the rights and freedoms to be guaranteed in the new Republic.

Additionally, articles 56, 61 and 75 of the Organic Law n°2015-26 of August 7, 2015 on the Fight Against Terrorism and the Prohibition of Money Laundering addresses the subject of personal data and when the use of personal data is permitted.

Tunisia became the 51st Member State of the Council of Europe Convention 108 on November 1, 2017 and its Additional Protocol No.181 on supervisory authorities and transborder data flows.

In March 2018, it introduced a new draft law on the protection of personal data in line with the new European GDPR in Parliament, however the law has not yet been passed.

In Tunisia, there is a whole legal arsenal relating to the processing of personal data.

In addition to the above-mentioned texts, there are also decisions rendered by the Instance such as:

- Decision n° 2 of October 6, 2017 on the processing of personal data in the political field;
- Decision n° 3 of September 5, 2018 establishing the countries that represent an adequate level of protection of personal data;
- Decision n° 4 of September 5, 2018 organizing personal health data; and
- Decision n° 5 of September 5, 2018 establishing the conditions and procedures for the installation of cameras and video surveillance.

DEFINITIONS

Definition of personal data

Article 4 of Act n° 2004-63 of July 27, 2004 defined personal data as all information, regardless of their origin or form, and which directly or indirectly, allows to identify or make identifiable, a natural person, with the exception of information related to public life, or considered as such by law.

Definition of sensitive personal data

Act n° 2004-63 of July 27, 2004 did not give a clear definition of sensitive personal data, but it listed some personal data that the processing of which is either prohibited, or would question the data subject’s prior consent or the national authority’s authorization.

The processing of personal data is prohibited when involving criminal history and proceedings, criminal prosecution, penalties, preventative measures or judicial history.

In addition, the processing of personal data which directly or indirectly concerns the following is also prohibited:

- Racial or genetic origins;
- Religious beliefs;
- Political opinions;
- Philosophical or union activism; or
- Health and scientific research.

Health data is defined by above-mentioned INPDP Decision No. 4 of September 5, 2018 as follows:

“*sensitive personal data, which concerns all information related to the physical, mental or psychological health situation of the natural person concerned, as well as his hereditary or acquired genetic characteristics that may characterize him or her and that may result especially from the analysis of a biopsy or physiotherapy services rendered to him or her and that may reveal such information*”.

NATIONAL DATA PROTECTION AUTHORITY

The National Authority for Protection of Personal Data (the Instance) was created by Decree n° 2007-3003 of November 27th, 2007. It Has several prerogatives and exercises several control operations that are organized by the decision n° 6 of the Instance dated October 6, 2019.

Any person may file a complaint with the INPDP regarding the violation of personal data committed by any entity.

The decisions of the Instance can be appealed before the Court of Appeal of Tunis and before the Court of Cassation.

REGISTRATION

Any processing of personal data shall be subject to a prior declaration filed at the headquarters of the National Authority for Protection of Personal Data, or by any other means leaving a written record.

- The declaration shall be made by the controller or his legal representative.
- The declaration does not exempt third parties from liability.
- The conditions and procedures for submitting the declaration shall be laid down by decree.
- The Commission may object to the processing of personal data within one month from when the declaration is accepted. (Article 7 of the 2004 Act).

The processing of personal data may be subject to prior authorization by the INDPD if it involves the processing of sensitive personal data, or in the case of transfer of personal data abroad, or if required by law.

The conditions and procedures for obtaining authorization are regulated by Decree n°. 2007-3004 dated 27 November 2007.

DATA PROTECTION OFFICERS

Under Tunisian law (Law n° 2004-63 dated July 27, 2004), there is no reference to Data Protection Officers.

Nevertheless, with regard to health data protection, Decision No. 4 of September 5, 2018 organizing personal health data, healthcare establishments must appoint a DPO.

For other types of sensitive personal data, it is preferable that each entity that processes personal data provides data subjects with an address of its DPO through which they can exercise their right of access to data and their right of opposition to their data processing.

COLLECTION & PROCESSING

The following principles generally apply to the processing of personal data:

- Personal data must be collected directly from the data subject;
- Personal data collected from third parties are permitted whenever the data subject, his heirs or his agent have provided their consent;
- The processing of personal data must respect human dignity, privacy and public liberties, and whatever its origin or its methods, it shall not harm the human rights protected by the laws and the rules in force. In every case, it is forbidden to use personal data with the aim of infringing people's rights or damaging their reputation;
- The collecting of personal data shall be exclusively carried out for lawful and clear purposes, and within the limits of the declared purposes. Any subsequent change of purpose must be the subject of a new declaration and a new consent from the person concerned; and
- Among the main prerequisites for the legitimate processing of personal data is the informed consent of the data subject, which means that the processing of personal data cannot be carried out without the express and written consent of the data subject. This consent shall be governed by the general rules of law if the data subject is incompetent or unauthorized or incompetent to sign.

The data subject or his agent is allowed to withdraw his consent, at any time during the processing.

Additionally, and in the spirit of child protection, Tunisian law has provided extra protection to personal data relating to children as this kind of data cannot be carried out without the consent of the child’s agent and after authorization of the juvenile and family court judge.

Finally, the consent provided for the processing of personal data under a specific given shall not apply to other forms or purposes.

Also, the data subject has the right of access, which means the right to consult all the personal data related to him as well as the right to correct, complete, rectify, update, modify, clarify or delete it, when it has been proved that it is inaccurate, equivocal or prohibited for processing by law, and also, the right to obtain a copy of the personal data in clear language, in accordance with the content of the recordings and in an understandable way in the case of automatic processing.

And finally, at anytime, the data subject, his heirs or his tutor has the right to object to the processing of personal data related to him for good, legitimate and serious reasons, except when the processing is scheduled by law or is required by the nature of the commitment. Furthermore, the data subject, his heirs or his tutor have the right to object to the communication to third parties of personal data related to him, in order to exploit it for promotional purpose. The objection immediately suspends the processing.

TRANSFER

The transfer of personal data is treated in the 5th Chapter of the 2004 Act on the protection of personal data (Articles 47 to 52), and is generally prohibited or subject to strict measures, including prior authorization (submitted to the National Authority for Protection of Personal Data), and the explicit consent of the person in question, which is mandatory. The transfer of personal data to a foreign country is prohibited whenever it may endanger public security or Tunisia's vital interests.

The international transfer of personal data may not take occur if the foreign country does not provide an adequate level of protection. In every case, the authorization of the Instance is required before the transfer of personal data. The Instance shall issue its decision within one month from the date of receipt of the application.

In its Decision No. 3 of September 5, 2018, the INPDP issued a non-exhaustive list of countries that represent an adequate level of protection of personal data, and to which the transfer is a priori possible, but always subject to obtaining the authorization of the INPDP.

SECURITY

Each person who carries out directly or by a third party the processing of personal data shall take all the required steps to ensure the safety of the data processing and prevent any third party from changing, modifying or consulting it without prior authorization of the data subject. (article 18 of Organic-Law n°2004-63 of July 27th 2004 on the protection of personal data).

The data controller must ensure that its subcontractor (if any) also implements all the organizational and technical measures necessary to ensure the protection of personal data against any kind of breach.

The National Authority for Protection of Personal Data is responsible for determining the proper measures and necessary safeguards in order to protect personal data.

In case of violation of the personal data protection legislation, in addition to the dissuasive actions it can take, it can also file a complaint with the public prosecutor to initiate criminal action.

If the personal data processed includes sensitive data such as health data, the data controller must subject its processing system to a periodic security audit in accordance with Legislative Decree no. 2023-17 of March 11, 2023 on cybersecurity.

BREACH NOTIFICATION

Under Tunisian Law, it is up to the person in question to make this kind of notification, or to its heirs and agents in certain circumstances.

Mandatory breach notification

The public prosecutor in the jurisdiction where the investigation takes place shall be informed by The National Authority for Protection of Personal Data of any offenses that it has detected.

ENFORCEMENT

The National Authority for Protection of Personal Data is legally mandated to ensure compliance with the provisions of the Law, but there is no information about cases where sanctions were applied to personal data infringements.

A draft bill on personal data has been considered by the Parliamentary Committee on Rights and Freedoms in the former Tunisian Parliament, which revolutionizes the existing Law, and when adopted, will be in correspond to the European standards for Data Protection, the bill has not yet been passed.

ELECTRONIC MARKETING

Electronic Marketing is regulated under Tunisian Law by The Electronic Exchanges and Electronic Commerce Law n° 2000-83 enacted on August 9, 2000.

This law is quite comprehensive and regulates the main aspects of this field. For instance:

- The preservation of the electronic document is as important as the preservation of the written document; and
- Each person using an electronic signature device shall:
  - Take minimum precautions to avoid illegitimate use of encryption elements or personal signature equipment; and
  - Inform the electronic certification service provider of any fraudulent use of his electronic signature.

For matters concerning personal data that have not been regulated by this law, the general protection regime should be applied.

Concerning the exercise of digital advertising, Law n°2004-63 requires the consent of the person concerned. In this context, article 30 of the said Law provides that :“*It is prohibited to use the processing of personal data for promotional purposes unless the data subject, his heir or his tutor gives his explicit and specific consent. This consent shall be governed by the general rules of law. The provisions of article 28 of the hereby Act shall apply if the data subject is a child*".

ONLINE PRIVACY

There is no specific mention to online privacy under the 2004 law on the Protection of Personal Data.

However, the same safeguards including restrictions and sanctions apply as well to online privacy under Tunisian Law.

Furthermore, it is prohibited to use the processing of personal data for promotional purposes unless the data subject, his heirs or his tutor gives his explicit and specific consent.

KEY CONTACTS

Mohamed Lotfi El Ajeri
Managing Partner
Al Ajeri Lawyers
T +(216) 71 288 251 – 71 287 238
mlelajeri@eal.tn

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

TURKEY

Last modified 5 September 2024

LAW

The main piece of legislation covering data protection in Turkey is the Law on the Protection of Personal Data No. 6698 dated April 7, 2016 (LPPD). The LPPD is primarily based on EU Directive 95/46/EC.

To date, the legislature has enacted several regulations to implement various aspects of the LPPD. The notable ones are mentioned below:

- Regulation on the Erasure, Destruction and Anonymizing of Personal Data (published in the Official Gazette dated October 28, 2017, numbered 30224);
- Regulation on the Working Procedures and Principles of Personal Data Protection Board (published in the Official Gazette dated November 16, 2017, numbered 30242);
- Regulation on the Registry of Data Controllers (published in the Official Gazette dated December 30, 2017, numbered 30286);
- Regulation on the Organization of Personal Data Protection Authority (published in the Official Gazette dated April 26, 2018, numbered 30403);
- The *Communiqué* on Procedures and Principles for Compliance with the Obligation to Inform (published in the Official Gazette dated March 10, 2018, numbered 30356);
- The *Communiqué* On The Principles And Procedures For The Request To Data Controller (published in the Official Gazette dated March 10, 2018, numbered 30356);
- The Decision of Data Protection Board, dated January 31, 2018, numbered 2018/10 on Adequate Measures to be taken by Data Controllers in Processing the Special Categories of Personal Data.

Certain general laws such as the Turkish Criminal Code no. 5237 and sector specific laws such as Electronic Communications Law No. 5809 also touch upon data protection and are mentioned below when relevant.

DEFINITIONS

Definition of personal data

In the LLPD, personal data is defined as “Any information relating to an identified or identifiable natural person.”

Definition of sensitive personal data

Sensitive personal data (Special Categories of Personal Data under the LPPD) is defined as "personal data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, clothing, membership of associations, foundations or trade unions, information related to health, sex life, previous criminal convictions and security measures, and biometric and genetic data.”

NATIONAL DATA PROTECTION AUTHORITY

The national data protection authority is the Kisisel Verileri Koruma Kurumu (Personal Data Protection Authority). The Personal Data Protection Authority’s decision-making body is Kisisel Verileri Koruma Kurulu (Personal Data Protection Board). The organizational structure of the Authority and the duties and powers of its bodies are regulated under the Regulation on the Organization of Personal Data Protection Authority and the Regulation on the Working Procedures and Principles of Personal Data Protection Board.

Kisisel Verileri Koruma Kurumu
Nasuh Akar Mah. Ziyabey Cad. 1407. Sok. No: 4
06520 Balgat-Çankaya / Ankara

T +90 312 216 5050

Website

kvkk.gov.tr

REGISTRATION

Pursuant to the LPPD and the Regulation on the Registry of Data Controllers, data controllers are required to enroll in the Registry of Data Controllers before proceeding with data processing.

The Regulation on the Registry of Data Controllers was published in the Official Gazette dated December 30, 2017, and entered into force on January 1, 2018. It regulates the establishment of a publicly accessible registry, which is to be held by the Personal Data Protection Authority and the procedures and principles concerning enrollment in the registry.

Under this Regulation, all data controllers are required to enroll in the Registry of Data Controllers before proceeding with data processing. However, the Personal Data Protection Board may bring an exception to the obligation of enrollment by taking into account the nature and number of personal data, purpose of processing personal data, and other objective criteria. Data controllers are not required to enroll in the Registry of Data Controllers in the following circumstances:

- The processing of personal data is required for criminal investigation or for prevention of a criminal offense;
- If the personal data being processed is already publicized by the data subject;
- If, based on the authority given by Law, personal data processing is required for disciplinary investigation or prosecution and execution of the supervision or regulation duties to be conducted by public institutions and organizations and professional organizations with public institution status; or
- If processing of personal data is required to protect the economic and financial interests of the State in relation to budget, tax and financial matters.

Over the past year, the Personal Data Protection Board has enumerated additional exceptions to enrollment obligation:

- Data controllers who process personal data by non-automatic means as a part of a filing system, lawyers, independent accountants and financial advisors;
- Natural or legal persons having less than 50 employees per annum and annual balance less than 25 million Liras and whose main field of activity is not processing special categories of personal data.

Data controllers who are non-resident in Turkey shall enroll in the registry through a representative they assign in Turkey. Legal persons in Turkey or Turkish citizens may be assigned as representatives for this purpose.

In addition, both legal entities resident in Turkey and the above-mentioned representatives of non-resident data controllers shall, as part of the enrollment procedure, appoint an individual to act as “contact person” for both the Personal Data Protection Authority and for data subjects.

Operations related to the Registry of Data Controllers shall be carried out through VERBIS (Data Controllers Registry Information System) by data controllers. The Personal Data Protection Authority, with its decision dated March 11, 2021, numbered 2021/238, had extended the dates for the registration through VERBIS until December 31, 2021.

Although the deadline has passed, it is still possible for local and foreign data controllers to register with VERBIS if the obligation arises or if the controller failed to register in time.

On August 15, 2022, the Data Protection Authority has started enforcement against foreign controllers that did not register within the deadline. Within the context of such enforcement the Data Protection Authority sent out letters to foreign controllers to request information as to reasons why the registration was not completed together with information on the number of users and global turnover to calculate the administrative fine.

Administrative fines of between TRY 189.245 - TRY 9.463.213 (approx. € 3.738 - € 296,245) may be imposed on data controllers breaching obligations regarding the Registry of Data Controllers.

Further, the DPA has the right to restrict the data processing activities of a data controller in cases of clear unlawfulness operation by a data controller and in theory, processing personal data without registering with the Registry of Data Controllers may lead to such restriction.

DATA PROTECTION OFFICERS

There is not yet a requirement in Turkey to appoint a data protection officer in the sense of GDPR. However, there is a requirement to appoint a local Representative for foreign controllers.

COLLECTION & PROCESSING

Pursuant to the LPPD, it is mandatory to comply with certain principles while collecting and processing personal data. In light of such principles collected personal data must be all of the following:

- Processed fairly and lawfully;
- Accurate and up-to-date;
- Processed for specific, explicit and legitimate purposes;
- Relevant, adequate and not excessive;
- Kept for a term necessary for purposes or for a term prescribed in relevant laws for which the data have been processed.

Further, in principle, personal data cannot be processed without being collected and processed with explicit consent of the data subject. However, the LPPD stipulates certain exceptions where consent is not required. These are:

- Processing is expressly permitted by law;
- Processing is necessary for protection of the life or physical integrity of the data subject or a third party, where the data subject is not physically or legally capable of giving consent;
- Processing personal data of the contractual parties is necessary for the conclusion or the performance of a contract;
- Processing is mandatory for the data controller to perform his / her legal obligation(s);
- Personal data has been made public by the data subject;
- Processing is necessary in order to assign, use or protect a right;
- Processing is necessary for the legitimate interests of data processor and this does not damage the rights of the data subject.

Pursuant to Article 10 of the LPPD, data controllers or their authorized persons have an obligation to inform data subjects during the collection of the personal data. The Communiqué on Procedures and Principles for Compliance with the Obligation to Inform published in the Official Gazette dated March 10, 2018, numbered 30356 sets forth the principles and procedures on the obligation to inform. As part of the collection of data from the data subject the controller is obliged to provide the data subject with the following information:

- Identity of the controller and of its representative, if any;

- Purposes of the processing for which the data is intended;
- Recipients of the data and the reasons for transfer;
- Process of collecting data and the legal grounds; and
- Rights of the data subject.

Where the data has not been obtained from the data subject, the controller shall provide the data subject with the above stated information as well as details of the categories of data concerned. According to the relevant *Communiqué*, the obligation to inform should be fulfilled within a reasonable time after collecting the personal data, or during the first contact if the personal data is obtained for communication purposes with the relevant persons, or at the very latest the time of the initial transfer if the personal data is to be transferred.

Processing of sensitive personal data without explicit consent of the data subject is generally forbidden, although sensitive data other than health and sexual life data can be processed without explicit consent of data subject if a law / legislation permits such processing. Under the LPPD, data controllers need to take adequate measures required for the processing of sensitive personal data and comply with the decisions and guides of the Personal Data Protection Board designating such adequate measures. See also Personal Data Protection Board Decision dated January 31, 2018, numbered 2018/10 on Adequate Measures to be taken by Data Controllers in Processing the Special Categories of Personal Data.

Health data and sexual life data can only be processed by natural persons who are under an oath of secrecy or by authorities for the purposes of protecting public health, preventive medicine, medical diagnosis, the provision of care and treatment services or planning, and the management and financing of healthcare services.

Deletion, destruction or anonymization of personal data

The Regulation on Deletion, Destruction or Anonymization of Personal Data ("Regulation on Deletion of Personal Data") was published in the Official Gazette dated October 28, 2017, and entered into force on January 1, 2018. This Regulation is crucially important for data controllers in terms of time limitations regarding deletion, destruction or anonymization of personal data.

Pursuant to the Regulation on Deletion of Personal Data, data controllers are required to prepare a personal data processing inventory and a personal data storage and destruction policy (Policy). Data controllers are also required to take measures to safeguard the data that they are processing, identify persons working in personal data storage and destruction processes, categorize personal data, store and destroy these data, and determine periodic destruction processes.

If the prerequisites for processing personal data provided under LPPD are not met, then the personal data must be deleted, destroyed or anonymized by the data controller (of its own accord or upon the application of related person). All actions related to the execution of this process must be recorded and these records shall be kept for at least three years.

In addition, if a data controller ceases to continue to meet the above conditions for processing personal data, then they must carry out a process of periodic destruction. Periodic destruction is the deletion, destruction or anonymization of personal data at recurring intervals specified in the relevant data controller's Policy. This period cannot exceed six months.

TRANSFER

The LPPD distinguishes between the transfer of personal data to third parties in Turkey and the transfer of personal data to third countries.

Transfer of personal data to third parties

In principle, personal data can be transferred to third parties with the explicit consent of the data subject. The conditions and exemptions applied to collection and processing of personal data also apply to the transfer of personal data to third parties.

Transfer of personal data to parties in third countries

In addition to the conditions and exemptions applied to the transfer of personal data to third parties, one of the following conditions shall exist for transfer of data to parties in third countries:

- The country to which personal data will be sent shall have sufficient level of protection;
- The data controllers in Turkey and in the target country shall undertake protection in writing and obtain the Personal Data Protection Board's permission; and
- Data controller shall sign BCRs published by the Personal Data Protection Board and obtain the approval of the Personal Data Protection Board.

The Personal Data Protection Board shall declare the countries having adequate level of protection. So far, the Personal Data Protection Board has not announced any country as adequate. However, the Personal Data Protection Board has announced the minimum clauses to be found in the undertakings of data controllers by setting out examples of undertaking where there is not an adequate level of protection in the country where personal data is transferred

In addition to the above, based on the announcement made by the Scientific Committee working towards amendments of the LPPD, the cross-border transfer rules will be updated and will be more in line with the GDPR. We are expecting the changes to occur within 2024.

SECURITY

In light of the provisions of the LPPD and consistent with the principles of good faith, those entrusted with personal data are expected to ensure protection of such data. Under the LPPD, the data controller is required to ensure that appropriate technical and organizational measures are taken to prevent all illegal processing and to ensure the data is not destroyed, lost, amended, disclosed or transferred without authority. Such measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected. Additionally, the data controller has to carry out the necessary inspections on its own institution or organization in order to ensure the implementation of the LPPD.

Data controllers and data processors shall not disclose any personal data in contradiction with the provisions of LPPD and shall not use any personal data for any purposes except for the purpose of processing. This obligation continues after leaving their institution.

In addition, the LPPD enables data subjects to apply to data controllers by various means in relation to their rights stated in Article 11. Data controllers have an obligation to take every necessary administrative and technical measure effectively to finalize these applications in accordance with the LPPD and in good faith. The Communiqué on Procedures and Principles for Application to Data Controller dated March 10, 2018, numbered 30356 outlines the procedures of application.

BREACH NOTIFICATION

There is no explicit definition of a data breach under Turkish Law. However, a breach can be defined as illegal acquisition of personal data by others / third parties.

The LPPD does not contain any thresholds for a notifiable breach. Therefore, all breaches (“illegal acquisition of personal data by others / third parties”) are notifiable to the Authority (within 72 hours) and to concerned data subjects (as soon as possible) without any criteria / threshold.

Under the DPL, controllers must notify the data subject and the Data Protection Authority in case of a data breach. The Data Protection Authority reserves the right to inform the public about the breach if it deems necessary.

While there is no specific time frame stipulated in the DPL, with the decision numbered 2019/10, which was published on February 15 2019, the Data Protection Authority stipulated the procedure for breach notifications, which can be found online.

Notification to the Data Protection Authority

Pursuant to Decision 2019/10, data controllers are required to notify the Data Protection Authority within 72 hours of becoming aware of a breach.

In cases where the notification cannot be sent within 72 hours, the causes for the delay must be sent as well.

Further, with the Decision 2019/10, the Data Protection Authority published the *Data Breach Notification Form*, which can be accessed here.

For all data breach notifications sent to the Data Protection Authority, the Data Breach Notification Form must be used. If it is not possible to fill out all of the information in the Data Breach Notification Form, a partially filled form may be sent to the Data Protection Authority. Therefore, gradual breach notification is possible.

The data breach notification sent to the Data Protection Authority can be sent via e-mail by sending the Data Breach Notification Form to ihlalbildirimi@kvkk.gov.tr with the subject “*Kişisel veri ihlali bildirimi*” or via the Data Protection Authority’s module.

Alternatively, the form can be sent by post to the Data Protection Authority’s address.

Notification to Data Subjects

There is no clear time frame stipulated for notification to data subjects. The **DPL** and the Decision 2019/10 require the data subjects to be notified “as soon as possible”. Notifications can be sent to data subjects directly if the data controller has their contact information. If not, any other appropriate way can be used, such as announcing the breach in data controller’s website.

Other requirements

Pursuant to Decision 2019/10, data controllers are required to prepare a “Data Breach Response Plan” which should specify who, within the organization, should be contacted in the event of a data breach. This person will be the primary person responsible for assessing the consequences of such a breach.

Further, there is a requirement to retain the records regarding (i) information on the data security breach, (ii) impacts of the breach, and (iii) measures taken, and to make these available for a possible assessment by the DPA.

ENFORCEMENT

Under the **DPL**, for the year 2023, the Board may apply administrative fines up to TRY 9.463.213 per breach in line with the following limitations. The amount of the administrative fines will be updated for 2024 based on the re-evaluation percentage to be published on the Official Gazette.

- Non-compliance with the information notice requirements: a fine between TRY 47.303 to TRY 946.308 (approx. € 1,480 to 29,624);
- Non-compliance with the data security obligations a fine between TRY 141.934 to TRY 9.463.213 (approx. € 4,443 to € 296,245);
- Non-compliance with Data Protection Authority orders / decisions: a fine between TRY 236.557 to TRY 9.463.213 (approx.€ 7,405 to 296,245); and
- Non-compliance with the Data Controllers’ Registry requirements: a fine between TRY 189.245 to TRY 9.463.213 (approx. € 5,924 to 296,245).

Further, under the Turkish Criminal Code, the following acts are subject to imprisonment:

- Persons who illegally collect personal data may be subject to imprisonment for a term of between one and three years. If the personal data is sensitive personal data, the offender may be subject to imprisonment for a term of between one and a half years to four and a half years.
- Persons who illegally transfer personal data or make personal data available to the public may be subject to imprisonment for a term of between two and four years.
- If any of the above criminal acts are committed by using the advantage or ease of a specific profession, or by a public officer using the authority given to him / her, the sanctions will be increased by 50%.
- Those responsible for the deletion of data following the expiry of the retention period, and who fail to do so, can be subject to imprisonment for a term of between one and two years.

ELECTRONIC MARKETING

The Law on Regulation of Electronic Trade was published in the Official Gazette on November 5, 2014 (Electronic Trade Law). The Electronic Trade Law came into force on May 1, 2015. Secondary legislation (The Regulation on Electronic Trade) was published in the Official Gazette on August 26, 2015, and came into force on the same date.

Pursuant to the Electronic Trade Law, commercial electronic communications (electronic marketing) can only be sent by if prior consent (opt-in) has been obtained from recipients. Such consent may be obtained in writing or through means of electronic communication, although if the consent is taken in physical from, must contain the recipient's signature. Commercial electronic communications can be sent to craftsman and merchants without obtaining prior consent. The commercial electronic communication must comply with the consent obtained from recipients, and must contain the identity of the service provider, contact information (such as email, SMS, telephone number, fax number (depending on the type of commercial electronic communication)), and, if sent on behalf of a third party, information about that third party.

Pursuant to Regulation on Commercial Communication and Commercial Electronic Messages, a registry named Message Management System (“**IYS**”) is established on January 4, 2020. Pursuant to the Regulation, all entities that wish to send commercial electronic messages (SMS, E-mail or calls) must register with IYS.

Commercial electronic messages are defined as “messages sent to electronic communication addresses (including audio calls) of recipients, for the purpose of promoting or advertising a product, service or business, and / or to increase the reputation of such through content including a greeting or a wish”.

The deadline for the service providers with 150.000 or more collected opt-ins to register with the IYS was December 31, 2020. The deadline for the service providers with 149.999 or less collected opt-ins was 31.05.2021.

Failure to register the collected opt-ins to IYS will result in all opt-ins consents to be invalid.

As of registration, opt-in consents can be obtained in writing or in any other electronic medium via IYS. It is required to report opt-in consents (which were not obtained via IYS) to IYS within 3 business days as of obtaining. All opt-in consents which were not reported to IYS will be deemed invalid.

Also, recipients will be able to submit their opt-out requests via IYS. Opt-out requests (which are not received via IYS) must be reported to IYS within three (3) business days. Sending commercial electronic messages must be stopped within three (3) business days as of receiving the opt-out request of the recipient.

Please note that obtaining opt-in consent is not necessary for commercial electronic messages if it is sent to merchants and craftsmen. However, they should also be registered with IYS and, it required to be checked whether they exercise their right to opt-out.

Consumers have the right to refuse a commercial electronic communication, and the service provider is obliged to allow the free transmission of the refusal. Commercial electronic communications to the recipient must cease within three business days of the receipt of refusal. For 2024, non-compliance with opt-in requirements is subject to administrative fines up to TRY 49.943 (approx. € 1,564).

Since electronic marketing activities include more and more use of personal data, the Electronic Trade Law and the LPPD often may be implicated at the same time. The Personal Data Protection Board Decision dated October 16, 2018 numbered 2018/119 states that commercial electronic communications such as advertisement notifications and marketing telephone calls also fall within the scope of the LPPD. However, this decision raised some questions regarding the application and enforcement of the Electronic Trade Law and LPPD at the same time, especially in relation to fines which may be imposed twice both according to the LPPD and the Electronic Trade Law.

ONLINE PRIVACY

There is no legislation in Turkey that specifically regulates privacy in respect of cookies and location data. However, Law No. 5651 on Regulating Broadcasting in the Internet and Fighting against Crimes Committed through Internet Broadcasting enables

Internet users to initiate prosecution in case of infringements of their personal rights. Further, various amendments were made to the Law No. 5651 on July 31, 2020. One of these amendments was adding the term *“social network provider”* and the obligations of the social network providers have been regulated within this scope.

Social network provider is defined as:

> "A natural or legal person who enables users to create, view, or share texts, images, voice, location, or other types of data for the purpose of social interaction."

The amendment requires foreign social network providers (companies that are not established in Turkey) which have daily access of 1.000.000 or more from Turkey to appoint a representative in Turkey. Also, the foreign social network providers must keep Turkish users’ (users from Turkey) personal data in Turkey within the scope of the Internet Law.

Failure to meet these requirements may result in administrative fines, limitation of bandwidth, and restriction of commercial activities (online marketing) of the social network provider. Moreover, with the recent amendments made in the Internet Law, social network providers may face an administrative fine up to 3% of their global turnover in cases of non-compliance.

Under the Regulation on Protection of Personal Data in the Electronic Communications Sector and Preservation of Privacy, an Operator cannot process traffic data for purposes other than those required for the purposes of their service. Traffic data shall be processed in accordance with the provisions of the relevant legislation for the purposes of traffic management, interconnection, billing, corruption detection and similar transactions or settlement of disputes. The processed and stored traffic data belonging to the subscriber / user shall be deleted or made anonymous after the completion of the required activity to process and store these data.

Traffic data may be processed if required for marketing electronic communication services or providing value added electronic communication services, provided that either it is anonymized, or relevant subscribers / users give their consent after being informed of the traffic data to be processed and the processing time.

Location data not qualifying as traffic data may be processed if required to provide value added electronic communication services, on the condition that it is anonymized or the relevant subscribers / users give their consent after being informed of the location data to be processed and of the purpose and duration of the processing.

Administrative fines of up to three percent of the net sales of the Operator in the previous calendar year shall be imposed if it fails to fulfill its obligation to process traffic data and location data.

KEY CONTACTS

Burak Özdağıstanli
Partner
Ozdagistanli Ekici Attorney Partnership
T +90 216 230 07 48
bozdagistanli@iptech-legal.com

Hatice Ekici Tağa
Partner
Ozdagistanli Ekici Attorney Partnership
T +90 216 230 07 48
hekici@iptech-legal.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

TURKMENISTAN

Last modified 23 December 2022

LAW

The Law of Turkmenistan No.519-V ‘On Information about Private Life and its Protection’ (the ‘Data Protection Law’) is the main and only law governing matters relating to collection and processing of personal data in Turkmenistan.

The Data Protection Law was enacted on 20 March 2017, ie after the adoption of the General Data Protection Regulation (the ‘GDPR’) and entered into force on 1 July 2017. In fact, the Data Protection Law partly reflects the rules and principles perpetuated in the GDPR. However, the similarities that can be discovered between the Data Protection Law and the GDPR are few and in most cases the Data Protection Law implements the simplified approach suggested by the GDPR.

DEFINITIONS

Article 1 of the Data Protection Law defines the term ‘personal data’ as ‘any kind of information, which relates to a certain individual, which is recorded on an electronic, paper or other medium’. In terms of accessibility, personal data can be divided into two types: public (such as telephone directory, social media, etc) and restricted. Publicly available personal data includes information, which is either freely accessible upon consent of the individual (owner of personal data) or exempted from confidentiality in accordance with the laws of Turkmenistan.

The Data Protection Law additionally introduces a term ‘biometric data’ that encompasses any information that reflects physical and biological characteristics of an individual (owner of personal data). The term is somewhat similar to the term ‘biometric data’ that is envisaged in the GDPR (Article 4(14)) but does not include any reference to physiological and behavioural characteristics.

Both personal data and biometric data are recognized as confidential under the Data Protection Law and collection and processing of such data must be limited to the purposes the data is collected for.

In Turkmenistan the Data Protection Law does not provide for a definition of sensitive personal data. It is directly prohibited to collect specific categories of personal data which, inter alia, includes data on nationality, skin colour, religious and political views, medical conditions, etc. Collection of such categories of personal data is permissible under the following circumstances:

- Receipt of a written consent of owner of personal information
- Such personal data is publicly available
- Collection of personal data is required for healthcare and health protection of an owner of such personal data
- Collection of personal data is performed by religious or non-commercial organization provided that the collected data would not be distributed without a prior written consent of owner of personal data
- Collection of personal data is required for implementation of justice and / or investigative activity

NATIONAL DATA PROTECTION AUTHORITY

There is no special national authority in the field of data protection policy.

REGISTRATION

No registration of a personal data database is required under the Data Protection Law.

DATA PROTECTION OFFICERS

No appointment of a data protection officer is required under the Data Protection Law.

COLLECTION & PROCESSING

Owner of personal data shall give consent on collection and processing of its personal data. Such consent can be delivered in written or electronic form or by virtue of any other secured means in compliance with Turkmen law.

Any such consent shall include the following information:

- Name (surname, name), address, ID document of an owner of personal data
- Name (surname, name) and the address of the data operator
- Purpose of collecting and processing personal data
- List of personal data to be collected and processed by the data operator
- List of actions related to personal data for the purpose of which the consent is given, a general description of the methods used to collect and process personal data
- Term of the given consent, as well as the procedure for its withdrawal

No consent is required for collection and processing of personal data for the following purposes:

- Investigatory activity
- Statistical analysis
- Life and health protection, protection of constitutional rights
- Implementation of international agreements of Turkmenistan, etc

TRANSFER

For the purposes of cross-border transfers of personal data, the relevant consent of owner of personal data is required. Since the Data Protection Law does not stipulate on whether this should be a separate consent, it is recommended to obtain such consent together with a general consent on collection and processing of personal data.

Please note that personal data transferred outside Turkmenistan shall also be stored in the territory of Turkmenistan. Personal data processed for the purpose of statistical and/or scientific analysis shall be de-personalized.

Data operator is not allowed to transfer personal data outside Turkmenistan to a third party by virtue of a contract on collection and/or processing of personal data.

SECURITY

Article 23 of the Data Protection Law stipulates that data operators shall implement a set of legal, organizational and technical measures to ensure personal data protection. Such measures shall:

- Uphold the rights to privacy, personal and family secrets
- Ensure integrity and security of personal data
- Confidentiality of personal data
- Allow owner of personal data to have guaranteed access to such personal data
- Prevent unauthorised collection and processing of personal data

Data operators are statutorily obliged to take any necessary and lawful measures to protect personal data and ensure:

- Prevention of unauthorized access to personal data
- Timely detection of unauthorized access to personal information
- No adverse effects of such unauthorized access to personal data

It is important to note that the obligation of the data operators, as well as any third party acquiring the personal data, to protect confidentiality of the acquired personal data, arises from the moment such data is collected and shall be effective until the moment such data is destroyed or depersonalized.

BREACH NOTIFICATION

Data Protection Law does not provide for any provisions regarding breach notification requirements. In other words, data operators are not obliged to notify the owners of personal data regarding any identified or potential confidentiality breach. However, the Data Protection Law envisages that data operators are obliged to block any personal data within one working day, if there is risk that a breach occurred.

ENFORCEMENT

General enforcement of the Data Protection Law is performed by the General Prosecutor’s Office. However, any suffered party may file a suit directly to a court.

ELECTRONIC MARKETING

Article 5(8) of the Law of Turkmenistan ‘On Advertising’ prohibits distribution of any information protected by the law (including personal data) for advertising purposes.

ONLINE PRIVACY

Data Protection Law provisions apply to online privacy as well. There are no other specific regulations that govern online privacy in Turkmenistan. Data operator shall refer to rules and regulations specified in the Data Protection Law.

KEY CONTACTS

Kamilla Khamraeva
Associate
Centil Law Firm
T +998 71 120 4778
kamilla.k@centil.law

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UAE - ABU DHABI GLOBAL MARKET FREE ZONE

Last modified 9 January 2024

LAW

Note: Please also see UAE – General, UAE – DIFC, UAE – DHCC.

The Abu Dhabi Global Market ("**ADGM**") is a financial freezone in Abu Dhabi emirate. The ADGM has powers to issue laws regarding its governance. On 14 February 2021 the ADGM issued the ADGM Data Protection Regulations 2021 ("**DPR**").

An important feature of the new framework is the establishment of an independent Office of Data Protection, headed by a Commissioner of Data Protection.

In order to assist businesses in understanding the requirements DPR, and how those should be applied to their activities, in August 2021 the Office of Data Protection issued a suite of eight guidance documents which cover the following topics:

1. General overview;
2. Data subject rights
3. Data protection by design and default, fees, record of Processing activities (“**ROPA**”), data protection officers (“**DPOs**”) and Processor obligations;
4. Data protection impact assessments (“**DPIAs**”);
5. Security of Processing and data breaches;
6. International transfers;
7. Codes of conduct and the role of the Commissioner of Data Protection and the Office of Data Protection; and
8. Individual Rights and Remedies.

DEFINITIONS

Definition of Controller

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

Definition of Processor

A natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

Definition of Data Subject

An identified or identifiable living natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Definition of Personal Data

Any information relating to a Data Subject.

Definition of Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

Definition of Processing

Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Definition of Special Categories of Personal Data

- Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- Genetic Data, Biometric Data for the purpose of uniquely identifying a natural person, Data Concerning Health or data concerning a natural person's sex life or sexual orientation; and
- Personal Data relating to criminal convictions and offences or related security measures.

NATIONAL DATA PROTECTION AUTHORITY

The Commissioner of Data Protection performs his functions with the support of the Office of Data Protection. Those functions include the following:

- exercising investigative powers, where necessary;
- monitoring and enforcing the application of the DPR;
- promote public awareness and understanding of the risks, rules, safeguards and rights in relation to Processing;
- advising and issuing opinions to the ADGM Board of Directors, Registration Authority, Financial Services Regulatory Authority, ADGM Courts, and other institutions and bodies on legislative and administrative measures relating to the protection individuals rights with regard to the Processing of Personal Data;
- promoting the awareness of Controllers and Processors of their obligations under the DPR. The Commissioner may also engage in outreach programmes to raise awareness and increase understanding DPR;
- providing the public with opportunities to provide views on the activities of the Office of Data Protection;
- handling complaints lodged by individuals, and investigating, to the extent appropriate, the complaint and informing the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation is necessary;
- cooperating with, including sharing information and provide mutual assistance to, other data protection authorities with a view to facilitating the effective enforcement of legislation for the protection of Personal Data worldwide;
- monitoring relevant developments insofar as they have an impact on the protection of Personal Data, in particular the development of information and communication technologies and business practices;
- adopting standard contractual clauses (as per Sections 26(6) and 42(2) DPR);
- publishing and maintaining a list as to the types of Processing operations which typically require a DPIA (as per Section 34 (4) DPR);
- approving codes of conduct and certification criteria (as per Sections 38(1) and 39(1) DPR);
- authorising contractual clauses and provisions referred to in Section 42(4) DPR;
- approving binding corporate rules pursuant to Section 43 DPR;

- issuing guidance and publishing standard forms (e.g. The August 2021 Guidance and the template DPIA);
- keeping records of non-compliance by those entities caught by the DPR, as well as any measures taken as a result of such non-compliance; and
- collecting data protection fees and renewal fees.

The contact details for the Office of Data Protection are as follows:

The Office of Data Protection
Authorities Building
ADGM Square
Al Maryah Island
Abu Dhabi
UAE

Email

Data.Protection@adgm.com

There is also a “Make An Enquiry” form available on the Office for Data Protection’s website.

REGISTRATION

Data protection fee

Section 24 DPR requires Controllers to pay a data protection fee to the Commissioner of Data Protection before, or as soon as reasonably practicable after, they start Processing Personal Data under the DPR.

It is also necessary to provide the Commissioner of Data Protection with:

- name and address (which, in the case of a registered company, will be its registered office); and
- Data Controllers must also establish and maintain records of any Personal Data Processing operations or set of such operations intended to secure a single purpose or several related purposes.

All licensed entities in the ADGM would have already provided much of the necessary information to the Commissioner of Data Protection during the company incorporation and registration Process. The date of incorporation is also the date the Controller may commence Processing Personal Data, such as the Personal Data of directors, shareholders and other statutory role holders. Each year, within one month of the expiry of the anniversary on which a Controller commenced Processing Personal Data under the DPR it is also necessary to pay the renewal fee.

The amounts payable are set out in the Data Protection Regulations 2021 (Fees) Rules 2021.

As per Section 28 DPR each Controller and Processor to which the DPR applies must maintain a record of Processing activities in writing. This can be in electronic form, but it does not necessarily need to be. The record of Processing activities must be made available to the Commissioner of Data Protection upon request.

DATA PROTECTION OFFICERS

Controllers and Processors must appoint a DPO where:

- the Processing is carried out by a public authority, except for courts acting in their judicial capacity;
- the core activities of the Controller or the Processor consist of Processing operations which, by virtue of their nature, scope and purposes, require regular and systematic monitoring of Data Subjects on a large scale; or
- the core activities of the Controller or the Processor consist of Processing on a large scale of special categories of Personal Data.

COLLECTION & PROCESSING

Data Controllers may Process Personal Data when any of the following conditions are met, as per Section 5(1) DPR:

- the Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes. There are detailed conditions for consent set out under Section 6 DPLs;
- Processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the Controller is subject under Applicable Law;
- Processing is necessary to protect the vital interests of the Data Subject or of another natural person;
- Processing is necessary for the performance of a task carried out by a public authority in the interests of ADGM, or in the exercise of (i) ADGM’s; (ii) the Financial Services Regulatory Authority’s; (iii) the ADGM Court’s; or (iv) the Registration Authority’s functions or in the exercise of official authority vested in the Controller under Applicable Law (as defined under the DPR);
- Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a Third Party, except where such interests are overridden by the interests or rights of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a Child.

Data Controllers may Process Special Categories of Personal Data when any of the following conditions are met:

- the Data Subject has given explicit Consent to the Processing of their Special Categories of Personal Data for one or more specified purposes;
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment law, provided that when the Processing is carried out, the Controller has an appropriate policy document in place in accordance with Section 7(3) DPR;
- Processing is necessary to protect vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving Consent;
- Processing is necessary for health purposes, including preventative or occupational medicine, the assessment of the working capacity of an employee, medical diagnosis, the provision of health care or treatment or the management of health care systems or services or pursuant to a contract with a health professional provided that Processing is by or under the responsibility of a health professional subject to the obligation of professional secrecy or duty of confidentiality;
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;
- Processing is necessary for Archiving and Research Purposes in accordance with Applicable Law;
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body including religious, cultural, educational, social or fraternal purposes or for other charitable purposes and on condition that the Processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data is not disclosed outside that body without the Consent of the Data Subjects;
- Processing relates to Personal Data which is intentionally made public by the Data Subject;
- Processing is required for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;

- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- Processing is necessary for reasons of substantial public interest, provided that (unless specified otherwise) the Controller has, when the Processing is carried out, an appropriate policy document in place in accordance with Section 7 (3), where it is necessary for:
    - the exercise of a function or requirement conferred on a person by Applicable Law;
    - the exercise of a function of the Board, Abu Dhabi or United Arab Emirate government;
    - the administration of justice;
    - equality of opportunity or treatment provided that the Processing does not, or is not likely to, cause substantial damage or substantial distress to an individual; and it does not relate to an individual who has given written notice to the Controller not to Process their Personal Data;
    - diversity at senior levels of organisations, where the Controller cannot reasonably be expected to obtain the Consent of the Data Subject and is not aware of the Data Subject withholding Consent provided that the Processing does not, or is not likely to, cause substantial damage or substantial distress to an individual;
    - the prevention or detection of an unlawful act or omission where the Processing must be carried out without the Consent of the Data Subject so as not to prejudice this purpose; and if the Processing relates to the disclosure of Personal Data to a relevant public authority an appropriate policy document in accordance with Section 7(3) need not be in place for the Processing to be lawful under these Regulations;
    - the protection of the members of the public against dishonesty, malpractice or other seriously improper conduct, unfitness or incompetence, mismanagement in the administration of a company, body or association, or failures in services provided by a company, body or association where the Processing must be carried out without the Consent of the Data Subject so as not to prejudice this purpose;
    - compliance with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has committed an unlawful act or omission, or been involved in dishonesty, malpractice or other seriously improper conduct where the Controller cannot reasonably be expected to obtain the Consent of the Data Subject to the Processing;
    - the prevention of fraud in connection with Processing of Personal Data as a member of, or in accordance with arrangements made by, an antifraud organisation;
    - the disclosure in good faith to an appropriate public authority regarding suspected terrorist financing, to identify terrorist property or in relation to suspected money laundering, in accordance with Applicable Law; or
    - the publication of a judgment or other decision of a court or tribunal or if the Processing is necessary for the purposes of publishing such a judgment or decision.

TRANSFER

International transfers

The DPR restricts the transfer of Personal Data out of the ADGM to a jurisdiction outside of the ADGM, or to an international organisation. Transfer is interpreted broadly and covers not only an act of sending, but also making available Personal Data to an individual or organisation in another jurisdiction. This includes transfer to onshore UAE based recipients.

There are various ways in which Personal Data can be legitimately transferred outside of the ADGM. Those are as follows:

1. transfer on the basis of an adequacy decision. The list of adequate jurisdictions can be found on the ADGM website. Note that these may be updated from time to time as the Commissioner will monitor for any changes in law which could

impact an adequacy decision. When making its assessment the Commissioner will take account of the factors set out at Section 41(2) DPR;

2. transfer on the basis of appropriate safeguards without the need for Commissioner approval for the transfer. Those include the following (provided always that the Controller or Processor has provided appropriate safeguards, and on condition that enforceable Data Subject rights and effective legal remedies for Data Subjects are available):

    i. a legally binding and enforceable instrument between public authorities;

    ii. binding corporate rules (BCRs);

    iii. standard data protection clauses adopted by the Commissioner of Data Protection (available online). Those are broadly based on the recently issued EU SCCs;

    iv. a Commissioner approved code of conduct pursuant to Section 37 DPR together with binding and enforceable commitments of the Controller or Processor in the jurisdiction outside of ADGM to apply the appropriate safeguards, including as regards Data Subjects' rights; or

    v. a Commissioner approved certification mechanism pursuant to Section 39 DPR together with binding and enforceable commitments of the Controller or Processor in the jurisdiction outside of ADGM to apply the appropriate safeguards, including as regards Data Subjects'.

The Commissioner does not require exporters relying on (i) – (v) above to conduct a detailed analysis of the laws of the importing jurisdiction, but recommends that exporters conduct due diligence on importing entities to ensure that they are capable of meeting their commitments under (i) – (v) above (as applicable).

3. where the Commissioner has given its approval to:

    i. contractual clauses between the Controller or Processor and the Controller, Processor or the recipient of the Personal Data outside of ADGM or the international organisation; and

    ii. provisions to be inserted into administrative arrangements, including regulatory memorandums of understanding between public authorities or domestic or international bodies which include enforceable and effective Data Subject rights; or

4. transfers made on the basis of the set out under Section 44 DPR (some of which are subject to additional qualifications):

    i. the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards;

    ii. the transfer is necessary for the performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request;

    iii. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person;

    iv. the transfer is necessary for important reasons of public interest;

    v. the transfer is required by law enforcement agencies of the UAE in accordance with Applicable Law (as defined under the DPR);

vi. the transfer is necessary for the establishment, exercise or defence of legal claims (including judicial, administrative, regulatory and out-of-court procedures); or

vii. the transfer is necessary in order to protect the vital interests of the Data Subject or of another person, where the Data Subject is physically or legally incapable of giving consent.

SECURITY

The obligation to provide appropriate technical and organisational (security) measures for Personal Data applies to both Controllers and Processors. The DPR do not specify any particular security measures, rather it is up to the organisation to judge what is appropriate in the circumstances taking into account:

- the state of the art (i.e. the current state of technological development as appropriate to the context including: industry practice; the type and scale of the Processing; and the availability of a product or solution in the market);
- the costs of implementation;
- the nature, scope, context and purposes of the Processing; and
- the likelihood and severity of risks to Data Subjects’ rights (in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data).

Controllers must only use Processors that can give sufficient guarantees they will implement appropriate technical and organisational measures to ensure their Processing will meet the requirements of the DPR and protect Data Subjects’ rights. Controllers are primarily responsible for overall compliance with the DPR, and for demonstrating that compliance. If this isn’t achieved, they may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures (see “Enforcement” below).

BREACH NOTIFICATION

In the event of a breach of any Personal Data held by a Data Processor, the Data Processor shall inform the Data Controller of the incident without undue delay after becoming aware of the Personal Data Breach (Section 32(2) DPR).

If a Data Controller becomes aware of a Personal Data Breach, the Data Controller must inform the Commissioner of Data Protection of the incident without undue delay, and where feasible, not later than 72 hours after becoming aware of it (Section 32 (1) DPR).

When the Personal Data Breach is likely to result in a high risk to the rights of natural persons, the Controller must communicate the Personal Data Breach to the Data Subject without undue delay.

ENFORCEMENT

Investigation and enforcement

The Commissioner has broad investigative powers under the DPR. Those include the power to:

- order, by notice in writing, Controllers and Processors to provide any information it reasonably requires for the performance of its duties and functions;

- initiate investigations into a Controller’s or Processor’s compliance with the DPR;

- it also has the power to access any equipment used to Process Personal Data (such as computers) and to take possession of any relevant documentation or information. The Commissioner must give written notice of the decision to investigate unless it believes that would likely result in the investigation being frustrated;

- carry out investigations in the form of data protection audits;

- carry out a review on certifications issued pursuant to Section 39 DPR;
- notify Controllers and Processors of any alleged contravention; and
- obtain, by notice in writing, from Controllers and Processors, access to all Personal Data and to all information reasonably necessary for the performance of its duties and functions.

From an enforcement standpoint, the Commissioner has the power to:

- issue and publish directions and warnings and make recommendations to Controllers and Processors that intended Processing operations are likely to contravene the provisions of the DPR;
- issue and publish directions and reprimands to Controllers and Processors where Processing operations have already contravened provisions of the DPR;
- order Controllers and Processors to comply with an individual's requests to exercise his or her rights pursuant to the DPR;
- order Controllers and Processors to bring Processing operations into compliance with the provisions of the DPR, where appropriate, in a specified manner and within a specified period;
- order a Controller to communicate a Personal Data Breach to the individual, where it has not done so already;
- impose a temporary or permanent limitation (including a ban) on Processing;
- order the rectification or erasure of Personal Data or restriction of Processing pursuant to Sections 14, 15 and 16 DPR and the notification of such actions to Recipients to whom the Personal Data has been disclosed, pursuant to Sections 15 (2) and 17 of the DPR;
- withdraw a certification if the requirements for the certification are not or are no longer met;
- impose an administrative fine pursuant to Section 55 of the DPR, in addition to, or instead of, any of the other measures set out under the DPR.

When considering whether to issue a fine the Commissioner will consider the circumstances on a case by case basis. For particularly serious breaches the Commissioner may well issue a fine and issue an order for the infringing party to resolve its infringement moving forwards;

- order the suspension of data flows to a recipient inside or outside of ADGM or to an international organisation; and
- where appropriate, refer contraventions DPR to the attention of the court and where appropriate, commence legal proceedings, in order to enforce the provisions DPR.

The DPR also provides a mechanism for Data Subjects to lodge complaints with the Commissioner (Section 57 DPR), and bring claims for compensation where they have suffered “*material or non-material damage*” as a result of a contravention DPR by a Controller or Processor (Section 59 DPR).

Notably the Commissioner has started to publish enforcement decisions, which are available upon the ADGM website.

ELECTRONIC MARKETING

According to Part 2 of the Commissioner’s Guidance, it is not always necessary to seek consent under the DPR to conduct direct marketing activities, such as sending marking emails. In many cases, it will be possible to rely upon legitimate interests (Section 5(1)(f) DPR) as the relevant legal basis for Processing. If relying on legitimate interests, it is important to ensure

that individuals are given the right to object both at the point at which their Personal Data is collected for direct marketing purposes, and within each communication (for example, by way of an “unsubscribe link” in an email). A pre-ticked box may be sufficient when offering the right to object at the point of data collection.

Whenever are relying on legitimate interests as the legal basis for Processing for direct marketing, consider whether the legitimate interests in conducting the marketing are overridden by the interests or rights of the Data Subject. Depending on the context of the direct marketing activities (for example, if the content of those marketing communications relates to products or services which are sensitive in some way, such as health related services), there may be instances where it will not be appropriate to rely on this as the relevant legal basis and consent would be more appropriate. Controllers must also ensure that they continue to meet their obligation to comply with the principles of transparency and fairness under Section 4 DPR by clearly describing their direct marketing activities in the applicable privacy notice.

ONLINE PRIVACY

The DPR does not contain specific provisions relating to online privacy, however, the broad provisions detailed above are likely to apply. Note that “online identifiers” fall within the definition of Personal Data. In addition, as UAE criminal law applies in the ADGM, the privacy principles laid out therein may apply (see UAE – General).

KEY CONTACTS

Eamon Holley
Special Consultant
T +971 4 438 6293
eamon.holley@dlapiper.com

Alex Mackay
Associate
T +971 4 438 6160
alex.mackay@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UAE - DUBAI (DIFC)

Last modified 9 January 2024

LAW

Note: Please also see UAE – General, UAE – ADGM, UAE – DHCC.

The Dubai International Financial Centre (“**DIFC**”) is a financial freezone in Dubai emirate. The DIFC has powers to issue laws regarding its governance. The DIFC Law No. 5 of 2020 on Data Protection Law (“**DPL**”) came into effect in July 2020.

In addition, alongside the DPL a new set of accompanying Data Protection Regulations (“**DPRs**”) were introduced. These were updated in 2023 to include regulations on processing via artificial intelligence systems.

DEFINITIONS

Definition of Data Subject

The identified or Identifiable Natural Person to whom Personal Data relates.

Definition of Personal Data

Any data referring to an “Identifiable Natural Person”.

Definition of Identifiable Natural Person

A natural living person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one (1) or more factors specific to his biological, physical, biometric, physiological, mental, genetic, economic, cultural or social identity.

Definition of Special Categories of Personal Data

Personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person.

Definition of Process, Processed, Processes and Processing

Any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage and archiving, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, transfer or otherwise making available, alignment or combination, restricting (meaning the marking of

stored Personal Data with the aim of limiting Processing of it in the future), erasure or destruction, but excluding operations or sets of operations performed on Personal Data by:

- a natural person in the course of a purely personal or household activity that has no connection to a commercial purpose; or
- law enforcement authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security.

Definition of Substantial Public Interest

Includes, but is not limited to:

- administration of justice, including criminal and regulatory investigations; and
- exercise of a function conferred on a person by Applicable Law.

NATIONAL DATA PROTECTION AUTHORITY

The Commissioner of Data Protection (“**Commissioner**”) is essentially the regulating body in the DIFC from a data protection standpoint.

The Commissioner of Data Protection
Dubai International Financial Centre Authority
Level 14, The Gate
P.O. Box 74777
Dubai
United Arab Emirates

commissioner@dp.difc.ae

Tel: +971 4 362 2222

REGISTRATION

Controllers and Processors are required to submit a notification to the Commissioner via the DIFC’s online portal (the “**Notification**”) (Article 14 (7) DPL) and to keep that up Notification to date.

The Notification must contain the following information:

- a general description of the Personal Data Processing being carried out;
- an explanation of the purpose for the Personal Data Processing;
- the Data Subjects or class of Data Subjects whose Personal Data is being Processed;
- a description of the class of Personal Data being Processed; and
- a statement of jurisdictions to which Personal Data will be transferred by the Controller, along with an indication as to whether the particular jurisdiction has been assessed as having an adequate level of protection for the purposes of articles 26 and 27 of the DPL.

The information set out within the Notification will be available on the DIFC’s public register.

Where an organisation is required to appoint a Data Protection Officer (see DPO), the DPO must complete an “Annual Assessment” in the form prescribed by the Commissioner.

DATA PROTECTION OFFICERS

Data Protection Officers (“**DPOs**”) are mandatory for:

- DIFC Bodies (as defined under the DPL, other than courts acting in their judicial capacity); and
- a Controller or Processor performing high risk Processing activities on a systematic or regular basis.

A Controller or Processor could also be required to appoint a DPO by the Commissioner.

A Group (defined under DPL) may appoint a single DPO provided that he is easily accessible to each entity in the Group. The DPO must reside in the UAE unless he is an individual employed within the organisation's Group and performs a similar function for the Group on an international basis.

In addition, if a Controller or Processor is not required to appoint a DPO, it must still clearly allocate responsibility for oversight and compliance with respect to data protection duties and obligations and provide details to the Commissioner (i.e. the person appointed, pursuant to the DPL, to monitor, ensure and enforce compliance with the DPL).

(Article 16 DPL)

COLLECTION & PROCESSING

Data Controllers may collect and Process Personal Data when any of the following conditions are met (set out under Article 10 DPL):

- a Data Subject has given consent, which complies with the comprehensive consent requirements set out under Article 12 of the DPL, to the Processing of that Personal Data for specific purposes;
- Processing is necessary for the performance of a contract to which a Data Subject is a party, or in order to take steps at the request of a Data Subject prior to entering into such contract;
- Processing is necessary for compliance with applicable law that a Controller is subject to;
- Processing is necessary in order to protect the vital interests of a Data Subject or of another natural person;
- Processing is necessary for:
    - performance of a task carried out by a DIFC Body in the interests of the DIFC;
    - exercise of a DIFC Body’s powers and functions; or
    - the exercise of powers or functions vested by a DIFC Body in a Third Party to whom Personal Data is disclosed by the DIFC Body; or
- Processing is necessary for the purpose of legitimate interests pursued by a Controller (or a third party to whom the Personal Data has been made available, subject to Article 13 of the DPL which sets out certain restrictions on the ability to rely upon legitimate interests), except where such interests are overridden by the interests or rights of a Data Subject.

Data controllers may collect and Process Special Categories of Personal Data when any of the following conditions are met (as per Article 11 DPL), in addition to establishing one of the legal bases under Article 10, set out above:

- a Data Subject has given explicit consent, which complies with the comprehensive consent requirements set out under Article 12 of the DPL, to the Processing of those Special Categories of Personal Data for one (1) or more specified purposes;
- Processing is necessary for the purpose of carrying out the obligations and exercising the specific rights of a Controller or a Data Subject in the context of the Data Subject's employment, including but not limited to recruitment, visa or work permit Processing, the performance of an employment contract, termination of employment, the conduct of proceedings

relating to employment and the administration of a pension, retirement or employee money purchase benefit scheme;

- Processing is necessary to protect the vital interests of a Data Subject or of another natural person, where the Data Subject is physically or legally incapable of giving consent;
- Processing is carried out by a foundation, association or any other non-profit-seeking body in the course of its legitimate activities, subject to appropriate assurances and provided that the Processing relates:
  - solely to the members or former members of such an entity; or
  - to other persons who have regular contact with such a body in connection with its purpose,

    and the Personal Data is not disclosed to a Third Party without the consent of a Data Subject;
- Processing relates to Personal Data that has been made public by a Data Subject;
- Processing is necessary for the establishment, exercise or defence of legal claims (including, without limitation, arbitration and other structured and commonly recognised alternative dispute resolution procedures, such as mediation) or is performed by the Court acting in its judicial capacity;
- Processing is necessary for compliance with a specific requirement of Applicable Law to which a Controller is subject, and in such circumstances the Controller must provide a Data Subject with clear notice of such Processing as soon as reasonably practicable unless the obligation in question prohibits such notice being given;
- Processing is necessary to comply with Applicable Law that applies to a Controller in relation to anti-money laundering or counter-terrorist financing obligations or the prevention, detection or prosecution of any crime;
- Processing is required for the purposes of preventive or occupational medicine, the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or the treatment or the management of health or social care systems and services, provided that the Personal Data is Processed by or under the responsibility of a health professional subject to an obligation of professional secrecy under applicable law or by another person also subject to an obligation of secrecy under applicable law;
- Processing is required for protecting members of the public against dishonesty, malpractice, incompetence or other improper conduct of persons providing banking, insurance, investment, management consultancy, information technology services, accounting or other services or commercial activities (either in person or indirectly by means of outsourcing), including any resulting financial loss; or
- Processing is proportional and necessary to protect a Data Subject from potential bias or inaccurate decision making, where such risk would be increased regardless of whether Special Category Personal Data is Processed.
- Processing is necessary for Substantial Public Interest reasons that are proportionate to the aim(s) pursued, respect the principles of data protection and provide for suitable and specific measures to safeguard the rights of the Data Subject.

Information Provision

Controllers are required to provide Data Subjects with certain information around how their Personal Data is processed in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information required to be provided is set out in detail under Part 5 of the DPL.

Where the Controller collects the Personal Data from the Data Subject, the information must be provided at the time of collection. (Article 29 DPL)

Where the Controller does not collect the Personal Data from the Data Subject, the Controller must provide the information:

- no longer than one (1) month from obtaining the Personal Data; or
- if the Personal Data is used for communicating with the Data Subject, no later than the first communication; or
- if a disclosure (including the making available for Processing) to a Processor or a third party is envisaged, no later than the time when the Personal Data is first disclosed.

(Article 30 DPL)

TRANSFER

As per Article 26 DPL, Personal Data may be transferred out of the DIFC:

- to a country or jurisdiction that has been determined to have adequate protections (available on the DIFC Commissioner for Data Protection website); or
- if it takes place in accordance with Article 27 DPL.

Article 27 DPL provides that:

A transfer or a set of transfers of Personal Data to a Third Country (i.e. Anywhere other than the DIFC, including onshore UAE) or an International Organisation (as defined within the DPL) may take place on condition that:

- the Controller or Processor in question has provided appropriate safeguards (as described in Article 27(2), set out below)), and on condition that enforceable Data Subject rights and effective legal remedies for Data Subjects are available;
- one of the specific derogations in Article 27(3) (set out below) applies; or
- the limited circumstances in Article 27(4) (set out below) apply.

Article 27 (2) DPL provides that the appropriate safeguards referred to at (a) above may be provided for by:

- a legally binding instrument between public authorities;
- Binding Corporate Rules (i.e. Personal Data protection policies and procedures, aggregated or incorporated in a single written document, which regulate the transfer of Personal Data between members of a Group, legally bind such members to comply, and which contain provisions for the protection of such Personal Data);
- standard data protection clauses adopted by the Commissioner (available on the DIFC website); The DIFC SCCs are a synthethised set of SCCs modelled on the EU Model Clauses and UK IDTA. They do not however take a modular approach;
- an approved code of conduct pursuant to Article 48 together with binding and enforceable commitments of the Controller or Processor in the third country or the International Organisation to apply the appropriate safeguards, including regarding a Data Subject’s rights; or
- an approved certification mechanism pursuant to Article 50 DPL together with binding and enforceable commitments of the Controller or Processor in the Third Country or the International Organisation to apply the appropriate safeguards, including regarding Data Subjects' rights.

Article 27 (3) DPL sets out the following derogations:

- a Data Subject has explicitly consented to a proposed transfer, after being informed of possible risks of such transfer due to the absence of an adequacy decision or appropriate safeguards;
- the transfer is necessary for the performance of a contract between a Data Subject and Controller or the implementation of pre-contractual measures taken in response to the Data Subject's request;
- the transfer is necessary for the conclusion or performance of a contract that is in the interest of a Data Subject between a Controller and a third party;
- the transfer is necessary for reasons of Substantial Public Interest;
- the transfer is necessary or legally required in the interests of the DIFC, including in the interests of the DIFC Bodies relating to the proper discharge of their functions;
- the transfer is necessary for the establishment, exercise or defence of a legal claim;
- the transfer is necessary in order to protect the vital interests of a Data Subject or of other persons where a Data Subject is physically or legally incapable of giving consent;
- the transfer is made in compliance with applicable law and data minimisation principles from a register that is:
    - intended to provide information to the public; and
    - open for viewing either by the public in general or by any person who can demonstrate a legitimate interest;
- subject to Article 28 DPL (which sets out the requirements for data sharing with public authorities), the transfer is:
    - The transfer is necessary for compliance with any obligation under applicable law to which the Controller is subject;
    - The transfer is made at the reasonable request of a regulator, police or other government agency or competent authority;
- the transfer is subject to international financial standards, the transfer is necessary to uphold the legitimate interests of a Controller recognised in international financial markets, except where such interests are overridden by the legitimate interests of the Data Subject relating to the Data Subject's particular situation; or
- the transfer is necessary to comply with applicable anti-money laundering or counter-terrorist financing obligations that apply to a Controller or Processor or for the prevention or detection of a crime.

Article 27(4) DPL provides that where a transfer could not be based on one of the aforementioned bases (including those at (a) –(k) (thereby making data transfers more flexible under the DPL), such transfer to a Third Country or an International Organisation may take place only if:

- the transfer is not repeating or part of a repetitive course of transfers;
- concerns only a limited number of Data Subjects;
- is necessary for the purposes of compelling legitimate interests pursued by the Controller that are not overridden by the interests or rights of the Data Subject; and
- the Controller has completed a documentary assessment of all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of Personal Data.

Under such circumstances the Controller is required to inform the Commissioner of any such transfer and to inform the Data Subject of the transfer and the compelling legitimate interests.

SECURITY

Controllers and Processors must implement appropriate technical and organisational measures to protect Personal Data against willful, negligent, accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of Processing, taking into account:

- the nature, scope, context and purpose of the Processing;
- the risks presented by the Processing to a relevant Data Subject; and
- prevailing information security good industry practice.

They must also review and update such measures, where necessary, to reflect legal, operational and technical developments.

(Article 14 (2) DPL)

BREACH NOTIFICATION

If there is a Personal Data breach that compromises a Data Subject's confidentiality, security or privacy, the data Controller must, as soon as practicable in the circumstances (note that unlike the GDPR there is no hard deadline), notify the Personal Data breach to the Commissioner. Such notifications must include, at a minimum, the following information:

- description of the nature of the Personal Data breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate amount of Personal Data records concerned;
- the name and contact details of the DPO or other contact point where more information can be obtained;
- a description of the likely consequences of the Personal Data breach; and
- describe the measures taken or proposed to be taken by the Controller to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide all of the information at (a) – (d) at the same time, the information may be provided in phases, as it becomes available.

In addition, Processors must notify Controllers without undue delay after becoming aware of a Personal Data breach.

Controllers and Processors must fully co-operate with any investigation of the Commissioner in relation to a Personal Data breach.

Controllers must also document in writing any Personal Data breaches, including the facts relating to the Personal Data breach, its effects and the remedial action taken. The information recorded must be sufficient to enable the Commissioner to verify compliance with the law and must be made available without delay on request.

(Article 41 DPL)

A Controller must make a notification to a Data Subject as soon as practicable in the circumstances (again, no hard deadline) where a Personal Data breach is likely to result in a high risk to the security or rights of a Data Subject. If there is an immediate risk of damage to the Data Subject, the Controller must promptly communicate with the affected Data Subject (for example, where his or her banking details are the subject of the breach).

Where a communication to the individual Data Subjects would involve disproportionate effort, a public communication or similar measure whereby the Data Subjects are informed in an “equally effective manner” will be sufficient.

Such notifications must include, at least, the information listed in (b) – (d) above, in clear and plain language. It must also, where possible, make recommendations for the Data Subject to mitigate against any potential adverse effects.

The Guidance to the DIFC DPL (“**Guidance**”) recommends that Controllers and Processors have in place an incident management policy which enables them to comply with the law in a timely fashion. It recommends clear incident classification as well as setting out the reporting requirements (including who to notify and when, with time being of the essence).

(Article 42 DPL)

ENFORCEMENT

The Commissioner has general powers to investigate and conduct inspections where it suspects that a Controller or Processor is not operating within the law.

Where it concludes that the Controller or Processor is not acting in compliance with the DPL, it has the power to:

- order it to do or refrain from doing any act or thing within such time as may be specified in the direction;
- order it to refrain from Processing any Personal Data specified in the direction or to refrain from Processing Personal Data for a purpose or in a manner specified in the direction;
- issue an administrative fine in an amount he considers appropriate but not exceeding the amount specified in Schedule 2 in respect of each contravention. The fines range from USD 10,000 to USD 100,000 and there are around 35 in total; and / or
- issue a general fine in an amount he considers appropriate and proportionate, taking into account the seriousness of the contravention and the risk of actual harm to any relevant Data Subject.

There is also a process built into the DPL and the DPRs for disputing any action taken by the Commissioner, with an ultimate right to challenge any action in court (Article 63 DPL).

Under the DPL Data Subjects also have the right to bring a claim for compensation where they suffer “material or non-material damage” by reason of any contravention of the law.

The DPL also contains provisions allowing Data Subjects to make compensation claims in relation to contraventions of the data protection law. Under the DPL, court proceedings can be initiated by the Commissioner as well as by Data Subjects.

The Commissioner has recently begun to publish certain limited information on its investigations and enforcement activities, including published decisions on infringements, which are available upon the DIFC website.

ELECTRONIC MARKETING

The DPL requires Controllers to provide Data Subjects with various pieces of information when they process their personal data (typically by way of a privacy notice, which must meet the detailed requirements set out Part 5 of the DPL), including whether the personal data will be used for direct marketing purposes.

Whilst consent is not expressly required (implying that one of the other legal bases can potentially be relied upon), Data Subjects do have the right to:

- be informed before Personal Data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object to such disclosures or uses; and
- where Personal Data is Processed for direct marketing purposes, object at any time to such Processing, including Profiling to the extent that it is related to such direct marketing.

(Article 34 DPL)

The Controller should also make clear in its Notification to the Commissioner that one of the purposes for which it Processes Personal Data is that of direct marketing.

ONLINE PRIVACY

Where a Controller is offering online services through a platform, the default privacy preferences of the platform must be set such that no more than the minimum Personal Data necessary to deliver or receive the relevant services is obtained or collected, and a Data Subject should be:

- prompted to actively select his privacy preferences on first use; and
- able to easily change such preferences.

(Article 14(4) DPL)

In addition, Controllers are to make available a minimum of two methods (which may include, by way of example, post, telephone, email or an online form) by which a Data Subject can contact the Controller to request to exercise his rights under the DPL. If the Controller maintains a website, at least one method of contact must be made available without charge via the website, without the need to submit data to create an account of any sort. (Article 40 DPL)

KEY CONTACTS

Eamon Holley
Special Consultant
T +971 4 438 6293
eamon.holley@dlapiper.com

Alex Mackay
Associate
T +971 4 438 6160
alex.mackay@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UAE - DUBAI HEALTH CARE CITY FREE ZONE

Last modified 2 January 2024

LAW

Note: Please also see UAE – General, UAE – DIFC, UAE – ADGM.

The Dubai Healthcare City ("**DHCC**"), a healthcare free zone in Dubai, implemented DHCC Health Data Protection Regulation No 7 of 2013 (which repealed and replaces the DHCC Data Protection regulation No. 7 of 2008) ("**HDPR**").

The HDPR regulates the protection of Patient Health Information, as opposed 'personal data'.

Note that as opposed to the ICT Health Law, which applies to entities across the UAE, including within freezones such as the DHCC (please see UAE – General), the DHCC HDPR only applies to those entities licensed within the DHCC and to patient information generated and stored therein.

In addition to the HDPR, the DHCC has also issued certain guidelines and standards, some of which have implications from a personal data protection standpoint, such as the DHCR Telehealth Standard (2017).

While the DHCC continues to have the HDPR available upon its website, the DHCC website also notes that “*All healthcare regulations in the Dubai Healthcare City free zone are managed by Dubai Health Authority. Please click here*[1] *for more information on all healthcare regulations related-matters*”.

Therefore, the actual application of the DHCC HDPR may still be subject to the interpretation and application of the Dubai Health Authority (“**DHA**”), including the application of the DHA’s own Policy for Health Data Protection and Confidentiality 2022.

1: See https://dhcc.ae/regulations/health-care-regulation

DEFINITIONS

Definition of Patient Health Information

Information about a patient, whether spoken, written, or in the form of an Electronic Record, that is created or received by any Licensee, that relates to the physical or mental health or condition of the patient, including the reports from any diagnostic procedures and information related to the payment for services.

Definition of Licensee

A Licensed Healthcare Professional, Licensed Complementary and Alternative Medicine Professional, a Licensed Healthcare Operator, an Approved Education Operator, an Approved Research Operator, a Licensed Commercial Company, or a Non-Clinical Operating Permit Holder; (essentially a healthcare professional working in the DHCC with access to Patient Health Information).

Definition of Process, Processed, Processes and Processing

Any operation or set of operations which is performed on Patient Health Information, whether or not by automatic means such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, erasure or destruction.

NATIONAL DATA PROTECTION AUTHORITY

The DHCC Board of Directors and the Executive Body of the Dubai Healthcare City Authority ("**DHCA**") are responsible for ensuring proper administration the HDPR and any Rules, Standards and Policies made under the HDPR.

The Centre for Healthcare Planning and Quality is responsible for the compliance and enforcement of the HDPR ("**CPQ**").

Dubai Healthcare City Authority - Regulatory
Tel: +971-4-3838300
Fax: +971-4-3838300
info@dhcr.gov.ae

REGISTRATION

Not applicable.

DATA PROTECTION OFFICERS

There is a requirement for each Licensee, to have one or more Data Protection Officers (**DPO**). The responsibilities of the Data Protection Officers include:

- the encouragement of compliance by the Licensee with the HDPR;
- dealing with requests made to the Licensee under the HDPR; and
- otherwise ensuring compliance by the Licensee with the provisions of the HDPR (section 40 HDPR).

COLLECTION & PROCESSING

Patient Health Information is not permitted to be collected by any Licensee, unless it is for a lawful purpose, and the collection is necessary for that purpose (article 27 HDPR). However, the meaning of lawful purpose is not defined in the HDPR.

The Patient Health Information should be collected from the patient directly, unless the Licensee believes on reasonable grounds that:

- the Patient concerned authorizes Collection of the information from someone else having been made aware of the matters set out in section 29(1);

- the Patient is unable to give his authority, and the Licensee having made the Patient’s Representative aware of the matters set out in section 29(1) Collects the Patient Health Information from the Representative or the Representative authorizes Collection from someone else;

- compliance would prejudice the:
    - interests of the Patient; or
    - purposes of collection; or

    - safety of any individual;

- compliance is not reasonably practicable in the circumstances of the particular case;

- the Collection is for the purpose of assembling a family or genetic history of a Patient and is collected directly from that Patient and / or the Patient’s Representative;

- the Patient Health Information is Publicly Available Information;

- the Patient Health Information:
    - shall not be used in a form in which the Patient is identified;
    - shall be used for statistical purposes and shall not be published in a form that could reasonably be expected to identify the Patient; or
    - shall be used for research purposes (for which approval by an ethics committee, if required, has been given) and shall not be published in a form that could reasonably be expected to identify the Patient; or

- non-compliance is necessary:
    - to avoid prejudice to the maintenance of the law including the prevention, detection, investigation, prosecution, and punishment of offences;
    - for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation) (section 28 HDPR).

TRANSFER

Patient Health Information may only be transferred to a third party located in a jurisdiction outside DHCC if:

1. an adequate level of protection for that Patient Health Information is ensured by the laws and regulations that are applicable to the third party; **and**
2. the transfer is either:
    - authorized by the Patient; or
    - necessary for the ongoing provision of Healthcare Services to the Patient.

A jurisdiction shall be considered to have an adequate level of protection if that jurisdiction is listed as an acceptable jurisdiction under the Dubai International Financial Center Data Protection Law No. 1 of 2007 or has the written approval of the Central Governance Board.

As noted above, DHA’s regulations regarding Policy for Health Data Protection and Confidentiality 2022 may now override the transfer provisions of the HDPR.

SECURITY

A Licensee is responsible for the security of its information systems and networks and should act in a timely and co-operative manner to prevent, detect and respond to security incidents. A Licensee is further required review and assess the security of information systems and networks and make appropriate modifications to security policies, practices, measure and procedures on a regular basis. Any security incidents must be disclosed to the CPU on a periodic basis.

A Licensee that holds Patient Health Information must maintain the security of the Patient Health Information, ensuring it is stored in a way that can be readily retrieved and easy removed or shared, as well as protecting the accuracy of the information. A Licensee if further responsible for ensuring reasonable safeguards are put in place to protect the Patient Health Information from loss, destruction, potential fire / water damage, tampering, theft, unauthorized access, use, modification, or disclosure (section 31, HDPR).

BREACH NOTIFICATION

There is no specific requirement set out in the DPL obliging a Licensee to inform the CPQ in the event of a breach. Licensees are required to inform the Customer Protection Unit (within CPU) on a periodic basis of any security incidents.

ENFORCEMENT

The CPQ is responsible for the compliance and enforcement of the HDPR and may delegate its powers and duties to any appropriate committee(s) constituted by it or to appropriate person(s) appointed by it (section 42 HDPR).

The powers, duties and functions of CPQ include: (a) conducting an audit of Patient Health Information when requested by a Licensee for the purpose of ascertaining whether or not the information is maintained in accordance with the HDPR; (b) monitoring the use of Personal Identifiers, and to reporting to the Executive Body from time to time on the results of that monitoring, including any recommendations relating to the need for, or desirability of taking regulatory, administrative, or other action to give protection, or better protection, to the Patient or the Licensee; and (c) monitoring compliance with the HDPR.

CPQ may require a Licensee to produce specified information or documents when requested in writing, in relation to the Processing of Patient Health Information of a complaint about an Interference with Patient Health Information. If the Licensee does not comply with the request, the CPQ may impose a Penalty as set out in a list to be published by the DHCA from time to time (section 42).

It does not appear that the DHCA have produced any further information on the penalties that apply in relation to a breach of HDPR. It is unclear how any breaches of the HDPR will be dealt with in the DHCC.

As noted above, the DHA’s interpretation and application of the HDPR may be relevant to the ultimate enforcement of the HDPR.

ELECTRONIC MARKETING

The HDPR does not contain specific provisions relating to electronic or direct marketing.

ONLINE PRIVACY

The HDPR does not contain specific provisions relating to online privacy, however, the broad provisions detailed above are likely to apply. In addition, as UAE criminal law applies in the DHCC, the privacy principles laid out therein may apply (see UAE – General).

KEY CONTACTS

Eamon Holley
Special Consultant
T +971 4 438 6293
eamon.holley@dlapiper.com

Alex Mackay
Associate
T +971 4 438 6160
alex.mackay@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UAE - GENERAL

Last modified 18 January 2024

LAW

Note: Please also see UAE – Dubai (DIFC), UAE – ADGM, UAE – DHCC.

Generally

As part of the 50th anniversary of its founding, the United Arab Emirates (“**UAE**”) has issued a set of sweeping legal reforms, including the much anticipated Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data Protection (“**PDPL**”), which was issued on 26 September 2021.

The executive regulations to the PDPL (“**Executive Regulations**”) were due to be published within six months of the issuance of the PDPL. However as of 31 December 2023, those have not yet been published. Once the Executive Regulations are issued, organisations have a further six months from their date of the issuance in which they can adjust operations to compliance with the PDPL.

Reassuringly, the PDPL does not contain any major divergences from other well-known data protection regimes, including the GDPR. In this regard we expect it will be welcomed by local, regional and international businesses, in particular those that rely heavily upon personal data and international personal data flows. International businesses with global privacy compliance programs should seek to expand those to cover the UAE and achieve some synergies. However, businesses that are not used to compliance with laws like the GDPR may find some of the new obligations challenging; for example, the PDPL introduces rights for individuals to access, rectify, correct, delete, restrict processing, request cessation of processing or transfer of data, and object to automated processing. There are also new requirements around transfers of data outside of the UAE and requirements to keep data secure, and to notify the new data protection regulator, and in some circumstances Data Subjects, of data breaches. The requirements regarding keeping data secure, and new data breach obligations, will definitely up the ante for businesses in the UAE to take cyber security seriously.

Territorial Scope

The PDPL applies to:

- processing of personal data of people residing in the UAE, or people having a business within the UAE;
- each Controller or Processor inside the UAE, irrespective of whether the personal data they process is of individuals inside or outside the UAE
- each Controller or Processor located outside the UAE, who carries out processing activities of Data Subjects that are inside the UAE.

Other data protection and privacy laws in the UAE

The PDPL keeps intact existing data protection and privacy laws within the UAE’s financial free zones, DIFC and ADGM, as well as the rules of the Dubai Health Care City, (links to our summaries are above) as well as applicable onshore laws regulating health data and banking and credit data. For this reason the data protection landscape in the UAE (and the wider GCC region) remains complex to navigate and somewhat fragmented, meaning that the application of the PDPL will need to be considered carefully.

There are several UAE federal level laws that contain various provisions in relation to privacy and the protection of personal data:

- United Arab Emirates Constitution of 1971;
- Federal Law 31 of 2021, on the Issuance of the Crimes and Penalties Law (“UAE Criminal Law”);
- Federal Decree Law No. 34 of 2021 on Combatting Rumors and Cybercrimes (“UAE Cyber Crime Law”);
- Federal Law by Decree No. 3 of 2003 as amended) On Organising the Telecommunications Sector (“UAE Telecommunications Law”) including several implementing regulations / policies enacted by the Telecommunications and Digital Government Regulatory Authority ('TDRA') in respect of data protection of telecoms consumers in the UAE.

There are also some federal level sectoral regulations in banking and finance, and in health, which should be considered.

The Central Bank Law (Federal Law No. 14 of 2018); Central Bank’s Consumer Protection Regulation issued under Central Bank Notice No. 444 of 2021, and related Central Bank Consumer Protection Standards issued under Notice No. 1158 of 2021 on Consumer Protection Standards

Article 120 of the Central Bank Law requires that all data and information related to customers should be considered confidential in nature.

On 31 December 2020 the UAE Central Bank published its Consumer Protection Regulation. It applies to all Central Bank Licensed Financial Institutions, which had one year in which to ensure their compliance.

Article 6 of the Consumer Protection Regulation requires that Licensed Financial Institutions must collect the minimal amount of Consumer Data and information needed in respect of their licensed activities and remain in compliance with all other related laws and treat Consumers' information relationships and business affairs as private and confidential.

The Central Bank Consumer Protection Standards outline detailed requirements regarding how Licensed Financial Institutions must comply with. These standards include Licensed Financial Institutions:

- having a proper Data Management Control Framework;
- using secure digital transaction processing and controls;
- designating responsibility and accountability for the data management and protection function to a senior position in management who reports directly to senior management;
- ensuring personal data is:
    - collected for a lawful urpose directly related to the Licensed Financial Activities of the Licensed Financial Institution;
    - adequate and not excessive in relation to the stated purpose; and
    - collected with appropriate security and protection measures against unauthorized or unlawful processing and accidental loss, destruction, or damage.
- notifying consumers prior to requesting consent to share consumer personal data;
- obtaining express consent of consumers prior to use or sharing of their data;
- retaining all personal data, documents, records and files securely for a minimum of 5 years;
- notifying the Central Bank of any material data breaches, losses, destruction or alteration when they occur.

Central Bank’s Stored Value Facilities Regulation

On 30 September 2020 the UAE Central Bank issued a new Stored Value Facilities Regulation (“SVF Regulation”), repealing and replacing the Regulatory Framework for Stored Values and Electronic Payment Systems it has issued in September

2016. While the SVF Regulation makes amendments to the licensing and enforcement regime for SVF (on onshore UAE only; it does not apply in, or affect, the DIFC and ADGM free zones), from a data protection perspective little has changed. The SVF Regulation applies to those providing Stored Value Facilities, which is now defined as *“a facility (other than cash) for or in relation to which a Customer, or another person on the Customer's behalf, pays a sum of money (including Money's Worth such as values, reward points, Crypto-Assets or Virtual Assets) to the issuer, whether directly or indirectly, in exchange for: (a) the storage of the value of that money (including Money's Worth such as values, reward points, Crypto-Assets or Virtual Assets), whether in whole or in part, on the facility; and (b) the “Relevant Undertaking”. SVF includes Device-based Stored Value Facility and Non-device based Stored Value Facility”.*

Article 10 of the SVF Regulation requires that licensees providing SVF services (**“SVFLicensee**”) must have in place adequate policies, measures and procedures to protect its information and accounting systems, databases, books and accounts, and other records and documents from unauthorized access, unauthorized retrieval, tampering and misuse.

An SVF Licensee must also adequately protect customer data (including customer identification and transaction records) which are required to be stored and maintained in the UAE. Such data can only be made available to the corresponding customer, the Central Bank, other regulatory authorities following prior approval of the Central Bank, or by a UAE court order. An SVF Licensee must store and retain all customer and transaction data for a period of five years from the date of the creation of the customer data, or longer if required by other laws.

Article 8 of the SVF Regulation requires that outsourcing arrangements must also contain adequate data protection and data handling controls.

Central Bank’s Retail Payment Services and Card Schemes Regulation

On 6 June 2021, the UAE Central Bank issued the Retail Payment Services and Card Schemes[1] Regulation (“Retail Services Regulation”). The Retail Services Regulation outline obligations and controls for the provision of Retail Payment Services and Card Schemes.

A Retail Payment Service includes any of the following: Payment Account Issuance Services; Payment Instrument Issuance Services; Merchant Acquiring Services; Payment Aggregation Services; Domestic Fund Transfer Services; Cross-border Fund Transfer Services; Payment Token Services; Payment Initiation Services; and Payment Account Information Services. The Retail Services Regulation does not apply to Stored Value Facilities.

Article 10 of the Retail Services Regulation requires that Payment Service Providers must have in place adequate policies, measures and procedures in relation to corporate governance, risk management, accounting and audit, record keeping, notification requirements and professional indemnity insurance. Amongst other things, article 10 requires the maintenance of confidential information, and that Payment Service Providers keep all necessary records on Personal and Payment Data for a period of 5 years.

Payment Service Providers must also put in place measures to ensure all business records can be restored in case they are lost, and that Retail Payment Service Users can access their own records in a timely manner. Payment Service Providers are also obligated to notify users of any loss in their records, and make reasonable effort to ensure that personal records are not wrongfully used.

Article 14 covers obligations towards Retail Payment Service Users, including protection of payment and personal data. Payment Service Providers to put in place policies and procedures to protect payment data and personal data and that Payment Service Providers only disclose Payment and Personal Data under the conditions outlined in the article.

The Retail Services Regulation further requires that Payment Service Providers store and maintain personal and payment data within the UAE, and must establish a safe and secure backup of all Personal and Payment Data in a separate location for the required period of 5 years.

Article 18 of the Retail Services Regulation considers Card Schemes, and place obligations on Card Scheme’s to notify the Central Bank in the case of a Data Breach no later than 72 hours after having become aware of such Data Breach.

ICT in Health Fields Law and Regulations, and Federal Ministerial Decision No 51 of 2021 Cases Allowing the Storage and Transfer of Medical Data and Information Out of the State

On 6 February 2018 Federal Law No. 2 of 2018 on the Use of the Information and Communication Technology (“**ICT** ”) in Health Fields (“**ICT in Health Fields Law**”) was issued. The primary purpose of the ICT in Health Fields Law is to establish a central electronic system of medical records for use within the health industry within the UAE.

Article 13 of the ICT in Health Fields Law states that the Health Information and data related to the health services provided in the UAE may not be stored, processed, generated or transferred outside the UAE, unless in the cases defined by virtue of a decision issued by the Health Authority of the relevant emirate in coordination with the Federal Ministry of Health.

The Minister of Health issued a decision on 28 April 2021 outlining the circumstances when Health Information can be transferred outside of the UAE.

The UAE ICT in Health Fields Law applies to all Competent Entities.

“Competent Entity” is defined as "*Any entity in the State providing medical services, health insurance or national health insurance services, brokerage services, claims management services or electronic services in the medical field of any entity related, whether directly or indirectly, to the implementation of the provisions hereof.*"

“Health Information” is defined as *“The health information that were processed and were given a visual, audible or readable indication, and that may be attributed to the health sector, whether related to the health or insurance facilities or entities or to the health services beneficiaries.”*

On 22 April 2020 the Federal Cabinet issued Cabinet Resolution No. 32 of 2020 concerning the Regulations Concerning the Use of the Information and Communications Technology in the Areas of Health (“**ICT in Health Fields Regulation s**”). The regulations provide further details, including on permission controls to access and use the central system, and on the storage and exchange of information on the central system.

Dubai Data Law

In December 2015 the Dubai Government published the Dubai Law No. 26 of 2015 on the Regulation of Data Dissemination and Exchange in the Emirate of Dubai, ("**Dubai Data Law**"). The purpose of the Dubai Data Law to collate and manage data that relates to the emirate of Dubai and, where appropriate, to publish it as “Open Data” or at least ensure that it is shared it between authorised persons. This law is considered unique as it is the only one in the world we are aware of that provides a government with the power to require designated private sector entities to provide to a government with information held by the company in relation to a city, for the purposes of making that information Open Data.

1: The Retail Services Regulation define Card Schemes as “*a single set of rules, practices and standards that enable a holder of a Payment Instrument to effect the execution of Card-based Payment Transactions within the State which is separated from any infrastructure of payment system that supports its operation, and includes the Card Scheme Governing Body. For the avoidance of doubt, a Card Scheme may be operated by a private or Public Sector Entity*”.

DEFINITIONS

The PDPL contains the following definitions.

Definition of Personal Data

“Personal Data” is defined as any data relating to an identified natural person, or one who can be identified directly or indirectly by way of linking data, using identifiers such as name, voice, picture, identification number, online identifier, geographic location, or one or more special features that express the physical, psychological, economic, cultural or social identity of such person. It also includes Sensitive Personal Data and Biometric Data.

Definition of Sensitive Personal Data

“Sensitive Personal Data” is defined as any data that directly or indirectly reveals a natural person's family, racial origin, political or philosophical opinions, religious beliefs, criminal records, biometric data, or any data related to the health of such person, such as his / her physical, psychological, mental, genetic or sexual condition, including information related to health care services provided thereto that reveals his / her health status.

Definition ofBiometric Data

“Biometric Data” is defined as Personal Data resulting from Processing, using a specific technique, relating to the physical, physiological or behavioral characteristics of a Data Subject, which allows or confirms the unique identification of the Data Subject, such as facial images or dactyloscopic data.

Definition of Processing

“Processing” is defined as any operation or set of operations which is performed on Personal Data using any electronic means, including Processing and other means. This process includes collection, storage, recording, organization, adaptation, alteration, circulation, modification, retrieval, exchange, sharing, use, or classification or disclosure of Personal Data by transmission, dissemination or distribution, or otherwise making it available, or aligning, combining, restricting, blocking, erasing or destroying Personal Data or creating models therefor.

Definition of Automated Processing

“Automated Processing” is defined as Processing that is carried out using an electronic program or system that is automatically operated, either completely independently without any human intervention, or partially independently with limited human supervision and intervention.

Definition of Controller

“Controller” is defined as an establishment or natural person who has Personal Data and who, given the nature of his / her activity, specifies the method, criteria and purpose of Processing such Personal Data, whether individually or jointly with other persons or establishments.

Definition of Processor

“Processor” is defined as an establishment or natural person who processes Personal Data on behalf of the Controller, as directed and instructed by the Controller.

Definition of Data Subject

“Data Subject” is defined as The natural person who is the subject of the Personal Data.

NATIONAL DATA PROTECTION AUTHORITY

At the date of writing this update the Data Office responsible for administering and enforcing the PDPL has not yet been established.

The UAE Central Bank is responsible for its Consumer Protection Regulation and Standards, the SVF Regulation and the Retail Services Regulation.

The Ministry of Health and Prevention is responsible for the ICT in Health Fields Law.

The Telecommunications and Digital Government Regulatory Authority (“**TDRA**”) is responsible for the regulation of its Consumer Protection Regulations.

REGISTRATION

There are no data protection registration requirements in the PDPL.

DATA PROTECTION OFFICERS

Processors and Controllers who are:

- conducting data processing which would cause a high risk to the confidentiality and privacy of the Data Subject’s personal data as a consequence of adopting new or data size-based technologies;
- conducting data processing will involve a systematic and comprehensive assessment of sensitive personal data, including profiling and automated processing; or
- processing large volumes of sensitive personal data will be processed,

will need to appoint a DPO.

The DPO can be a staff member or someone working on a service contract and does not necessarily need to be located in the UAE.

COLLECTION & PROCESSING

Data Protection Controls (Article 5)

Under the PDPL, Personal Data must be processed according to the following controls:

- Processing must be made in a fair, transparent and lawful manner;
- Personal Data must be collected for a specific and clear purpose, and may not be processed at any subsequent time in a manner incompatible with that purpose. However, Personal Data may be processed if the purpose of Processing is similar or close to the purpose for which such data is collected;
- Personal Data must be sufficient for and limited to the purpose for which the Processing is made;
- Personal Data must be accurate and correct and must be updated whenever necessary;
- Appropriate measures and procedures must be in place to ensure erasure or correction of incorrect Personal Data;
- Personal Data must be kept securely and protected from any breach, infringement, or illegal or unauthorized Processing by establishing and applying appropriate technical and organizational measures and procedures in accordance with the laws and legislation in force in this regard;
- Personal Data may not be kept after fulfilling the purpose of Processing thereof. It may only be kept in the event that the identity of the Data Subject is anonymized using the “Anonymization” feature;
- Any other controls set by the Executive Regulations of this Decree Law.

Legal Bases for Processing (Article 4)

The PDPL prohibits Processing Personal Data without the consent of the Data Subject, except in the following cases:

- if the Processing is necessary for the Controller or Data Subject to fulfill his / her obligations and exercise his / her legally established rights in the field of employment, social security or laws on social protection, to the extent permitted by those laws;
- if the Processing is necessary to perform a contract to which the Data Subject is a party or to take, at the request of the Data Subject, procedures for concluding, amending or terminating a contract;
- if the Processing is necessary to protect the interests of the Data Subject;
- if the Processing is for Personal Data that has become available and known to the public by an act of the Data Subject;
- if the Processing is necessary to protect the public interest;
- if the Processing is necessary to initiate or defend against any actions to claim rights or legal proceedings, or related to judicial or security procedures;
- if the Processing is necessary for the purposes of occupational or preventive medicine, for assessment of the working capacity of an employee, medical diagnosis, provision of health or social care, treatment or health insurance services, or management of health or social care systems and services, in accordance with the legislation in force in the State;

- if the Processing is necessary to protect public health, including the protection from communicable diseases and epidemics, or for the purposes of ensuring the safety and quality of health care, medicines, drugs and medical devices, in accordance with the legislation in force in the State;
- if the Processing is necessary for archival purposes or for scientific, historical and statistical studies, in accordance with the legislation in force in the State;
- if the Processing is necessary to fulfill obligations imposed by other laws of the State on Controllers;
- any other cases set by the Executive Regulations.

Processing of Sensitive Personal Data

Unlike the GDPR, the PDPL does not impose more stringent controls around processing of Sensitive Personal Data, however if a Controller or Processor is Processing that involves a systematic and comprehensive assessment of Sensitive Personal Data, including profiling and automated processing, or if the Processing will be made on a large amount of Sensitive Personal Data, then the Controller or Processor must appoint a Data Protection Officer (Article 10).

Article 21 also requires that DPIAs be conducted before Processing that will use any of the modern technologies that would pose a high risk to the privacy and confidentiality of the Personal Data of the Data Subject, if the Processing will be made on a large amount of Sensitive Personal Data (Article 21)

Transparency (Privacy Notices)

The PDPL contains a broad obligation to process personal data in a transparent manner. This obligation is not placed specifically on either Controllers or Processors, so it can be assumed that it is intended to apply to both. Under other data protection laws, the general transparency obligation is often tied to a clear obligation to provide a privacy notice to Data Subjects which meets prescriptive content requirements. The PDPL does (yet) not have an express provision regarding this (although it is possible that the Executive Regulations may do). However, the PDPL does give Data Subjects a detailed right of access (without charge) to the types of information which would ordinarily be contained in a privacy notice. Moreover, per Article 13 of the PDPL, the Controller is required to, in all cases and prior to the commencement of processing, provide Data Subjects with information regarding:

- the purposes of the processing;
- the targeted sectors or establishments with whom the personal data will be shared, both within and outside the UAE; and
- the protection measures for cross-border processing.

Therefore, in practice, Controllers may ultimately consider publishing privacy notices that contain, at least in broad terms, the information that the Data Subject is entitled to seek under the PDPL.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data replicating those in the EU GDPR. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right to obtain information (‘data access’) (Article 13)

A Data Subject is entitled to request access to and obtain the following information without charge:

- the types of his / her Personal Data that is processed;
- purposes of Processing;
- decisions made based on Automated Processing, including Profiling;
- targeted sectors or establishments with which his / her Personal Data is to be shared, whether inside or outside the State;
- controls and standards for the periods of storing and keeping his / her Personal Data;
- procedures for correcting, erasing or limiting the Processing and objection to his / her personal data;
- protection measures for Cross-Border Processing;

- procedures to be taken in the event of a breach or infringement of his / her Personal Data, especially if the breach or infringement poses a direct and serious threat to the privacy and confidentiality of his / her Personal Data;
- the process of filing complaints with the Data Office.

Right to request Personal Data transfer (‘data portability’) (Article 14)

The Data Subject has the right to obtain his / her Personal Data provided to the Controller for Processing in a structured and machine-readable manner, so long as the Processing is based on the Consent of the Data Subject or is necessary for the fulfillment of a contractual obligation and is made by automated means.

The Data Subject has the right to request the transfer of his / her Personal Data to another Controller whenever this is technically feasible.

Right to correction or erasure ('right to be forgotten') (Article 15)

The Data Subject has the right to request the correction or completion of his / her inaccurate Personal Data held with the Controller, and has the right to request the erasure of his / her Personal Data held with the Controller in any of the following cases:

- if his / her Personal Data is no longer required for the purposes for which it is collected or processed;
- if the Data Subject withdraws his / her Consent on which the Processing is based;
- if the Data Subject objects to the Processing or if there are no legitimate reasons for the Controller to continue the Processing;
- if his / her Personal Data is processed in violation of the provisions hereof and the legislation in force, and the erasure process is necessary to comply with the applicable legislation and approved standards in this regard.

Right to restriction of Processing (Article 16)

The Data Subject has the right to oblige the Controller to restrict and stop Processing in any of the following cases:

- if the Data Subject objects to the accuracy of his / her Personal Data, in which case the Processing shall be restricted to a specific period allowing the Controller to verify accuracy of the data;
- if the Data Subject objects to the Processing of his / her Personal Data in violation of the agreed purposes;
- if the Processing is made in violation of the provisions hereof and the legislation in force.

The Data Subject has the right to request the Controller to continue to keep his / her Personal Data after fulfillment of the purposes of Processing, if such data is necessary to complete procedures related to claiming or defending rights and legal proceedings.

Right to stop Processing (Article 17)

The Data Subject has the right to object to and stop the Processing of his / her Personal Data in any of the following cases:

- if the Processing is for direct marketing purposes, including Profiling related to direct marketing;
- if the Processing is for the purposes of conducting statistical surveys, unless the Processing is necessary to achieve the public interest;
- if the Processing is in violation the controls referred to in Article 5 (referred to above)

The right not to be subject to automated decision making, including profiling (Article 18)

The Data Subject has the right to object to decisions issued with respect to Automated Processing that have legal consequences or seriously affect the Data Subject, including Profiling. However, the Data Subject may not object to the decisions issued with respect to Automated Processing in the following cases:

- if the Automated Processing is included in the terms of the contract entered into between the Data Subject and Controller;

- if the Automated Processing is necessary according to other legislation in force in the State;
- if the Data Subject has given his / her prior Consent on the Automated Processing.

TRANSFER

Data transfers out of the UAE may be subject to different laws.

The PDPL imposes limitations on the international transfer of Personal Data to outside of the UAE. Similar to the concept of the “adequate jurisdictions” in the EU, the Data Office is expected to approve certain territories as having sufficient provisions, measures, controls, requirements and rules for protecting privacy and confidentiality of personal data. There are also various other exceptions which exporters can rely on, although further details are awaited from the Data Office.

Article 10 of the SVF Regulation requires that customer data (including customer identification and transaction records) are required to be stored and maintained in the UAE.

Article 13 of the ICT in Health Fields Law requires that Health Information and data related to the health services provided in the UAE may not be stored, processed, generated or transferred outside the UAE, unless in the cases defined by virtue of a decision issued by the Health Authority of the relevant emirate in coordination with the Federal Ministry of Health. Federal Ministerial Decision No 51 of 2021 Cases Allowing the Storage and Transfer of Medical Data and Information Out of the State, outlines the circumstances in which such Health Information may be transferred outside of the UAE. The Federal level also requirements need to be considered against various Emirate level policies, procedures and guidance documents which, depending upon the location of the relevant parties, patients and the nature of the activities being performed may also impact the collection, processing and international transfer of health information.

In addition, in circumstances where telecommunications service providers provide subscriber information to affiliates or third parties directly involved in the supply of the telecommunications services ordered by a subscriber, the third parties are required to take all reasonable and appropriate measures to protect the confidentiality and security of the subscriber information, and use such information only as needed for the provision of the requested services. Telecommunications service providers are required to ensure that the contracts between them and any affiliate or third party holds the other party responsible for the privacy and protection of the subscriber’s information (TDRA Consumer Protection Regulations v1.5, Article 20.8).

SECURITY

The PDPL imposes strict requirements around data security. Controllers and Processors are required to put in place sufficient technical and authorised measures to protect and secure Personal Data, preserve its confidentiality and privacy, and ensuring that such personal data is not breached, destroyed or altered. The measures which must be taken need to take into account the nature, scope and purposes of processing and the possibility of risks to the confidentiality and privacy of the Data Subject’ s Personal Data. Put simply, this means the higher the risk of harm to the Data Subject and / or the higher the likelihood of a breach, the greater the steps to secure personal data that need to be taken.

The UAE's Federal Cabinet has issued Resolution No. 21 of 2013, concerning the Regulation of Information Security in Federal Authorities. Although it applies to information security within UAE federal government bodies, the requirements of this resolution might be passed on to contractors providing services to Federal government bodies when they are entering into service supply agreements with such bodies. Similarly, contractors to emirate level government bodies may need to require with emirate government security standards. Examples, include the Information Security Regulations of the Dubai Electronic Security Center.

Article 20.1 of the TDRA Consumer Protection Regulations v1.5 requires telecommunications service providers to *“take all reasonable and appropriate measures to prevent the unauthorised disclosure or the unauthorised use of subscriber information”*. Article 20.3 further stipulates that telecommunications service providers must take *“all reasonable measures to protect the privacy of Subscriber Information that it maintains in its files, whether electronic or paper for”*, and that *“reliable security measures”* should be employed.

The UAE Cyber Crime Law focuses on offences related to accessing data without permission and/or illegally (Articles 2 and 3), including financial information (e.g. credit card information or bank account information) (Articles 12 and 13).

Based on the above, best practice from a UAE law perspective would be to take appropriate technical security measures against unauthorised or unlawful processing of, and against accidental disclosure of, personal data. The measures taken must ensure a level of security adequate enough to minimise the risk of liability arising out of a claim for breach of privacy made by a Data Subject.

BREACH NOTIFICATION

Article 9 of the PDPL requires that the Controller shall, immediately upon becoming aware of any infringement or breach of the Personal Data of the Data Subject that would prejudice the privacy, confidentiality and security of such data, report such infringement or breach and the results of the investigation to the Office within such period and in accordance with such procedures and conditions as set by the Executive Regulations. At the date of writing this update, the Executive Regulations have not yet been published.

ENFORCEMENT

The PDPL does not specify penalties, but notes that the Cabinet shall, based on the proposal of the Office General Manager, issue a decision specifying the acts that constitute a violation of the provisions of this Decree Law and the Executive Regulations thereof and the administrative penalties to be imposed.

Despite this there remain possible methods of enforcement of other UAE privacy laws:

1. Where the unauthorised disclosure of personal data results in a breach of the Penal Code

The Public Prosecutor in the Emirate where:

- the party suspected of the breach (‘Offender’) resides; or
- the disclosure occurred,

will have jurisdiction over a Data Subject’s complaint.

If after concluding investigations with the police, the Public Prosecutor is satisfied with the evidence compiled, charges may be brought against the suspect.

The case would then be transferred to the Criminal Courts of First Instance. The Data Subject may attach a civil claim to the criminal proceedings before the Courts have ruled on the case.

Pursuant to Article 432 of the Criminal Law, if the Courts find a suspect who by virtue of his profession, occupation, status, or specialisation has access to a secret but discloses such secret in other than the cases permitted by Law, or who uses such secret for his own benefit or the benefit of another person, unless such disclosure or use is authorised by the concerned person, may be penalized by a fine of at least UAE Dirhams 20,000 (the fine is determined by the Courts) and / or an imprisonment for at least one year.

Similarly, pursuant to Article 431 of the Criminal Law a punishment of *“a jail sentence and a fine”* shall be inflicted on any person who interferes with the right to privacy and family life of individual by:

- eavesdropping, or recording, or transmitting, through a device of any type, conversations done privately or by phone or any other device.
- taking or transmitting, through a device of any type, pictures of any person in private,

unless legally permitted or with the individual’s consent.

When ruling on the criminal case, the Criminal Courts would usually transfer a civil claim made by the Data Subject to the Civil Courts of First Instance for further consideration. The Data Subject would need to prove the losses he / she has suffered as a direct result of the disclosure of his / her personal data before the Civil Courts in order for damages to be awarded.

2. Where the unauthorised disclosure of personal data results in a breach of the Cyber Crime Law

The police in each Emirate have developed specialised cybercrime units to handle complaints that relate to breaches of the Cyber Crime Law.

As above, the cybercrime unit in the Emirate where:

- the Offender resides; or
- where the disclosure occurred,

will have jurisdiction over a Data Subject’s complaint.

The cybercrime unit would investigate the case and decide whether or not to refer it to the Public Prosecutor in the same Emirate. If the case is referred and the Public Prosecutor is satisfied with the findings of the cybercrime unit, charges would be brought against the suspect. The same procedure identified above is then followed before the Courts.

If found guilty of an offence under the Cyber Crime Law, the punishment an Offender can receive varies depending on the nature of the crime. Punishments range from temporary detention, a minimum prison sentence of between six months or one year and / or a fine between AED 150,000 and 5,000,000 (Articles 2, 3, 4, 6, 7, 8 and 45 of the Cyber Crime Law). Notably, Article 13 of the Federal Decree Law No. 34 of 2021 on Combatting Rumors and Cybercrimes provides that *“Everyone employs information technology or an information technology method to* ***collect, keep or process personal data and information of the nationals or the residents in the state in violation of the legislations in force in the state*** *shall be sentenced to detention and/or to pay fine of not less than (50,000) fifty thousand Dirhams and not more than (500,000) five hundred thousand Dirhams.”* As such, it is likely that this penalty may apply for breaches of the PDPL. If found guilty of an attempt to commit any of the relevant offences under the Cyber Crime Law, the punishment is half the penalty prescribed for the full crime (Article 57).

3. Where the unauthorised disclosure or transfer of personal data results in a breach of the Central Bank’s Consumer Protection Regulation, Retail Services Regulation or SVF Regulation

The Central Bank may issue administrative and / or financial penalties against Licensed Financial Institutions, SVF Licensees and Payment Service Providers at their discretion. In the case of the Consumer Protection Regulation they may include fines, replacing or restricting the powers of Senior Management or Members of the Board.

4. Where the unauthorised disclosure of personal data results in a breach of the UAE Telecommunications Law and Policies

The TDRA is responsible for overseeing the enforcement of the UAE Telecommunications Law and in this regard may rely on the Police and Public Prosecutor in the Emirate where, either:

- the breach has occurred; or
- where the suspect resides.

Where a licensed telecommunications service provider has breached the law, the subscriber / Data Subject generally needs to complain first to the service provider about the breach, though a direct approach to the TDRA may be accepted by the them at their discretion (Article 15.11.1 of the TDRA Consumer Protection Regulations v1.5).

The subscriber's complaint needs to be submitted to the TDRA within three months of the date when the service provider last took action . This three months requirement may be waived subject to the discretion of the TDRA (Article 15.11.1 of the TDRA Consumer Protection Regulations v1.5).

After examining the complaint the TDRA may direct the service provider 'to undertake any remedy deemed reasonable and appropriate' (Article 15.11.5 of the TDRA Consumer Protection Regulations v1.5).

ELECTRONIC MARKETING

There are no general laws in the UAE law covering electronic marketing, however the TDRA has issued a regulation governing telecommunications licensees' electronic communications with subscribers, as well as how they should monitor spam passing through their networks. Article 6 of the Cyber Crime Law and Article 20.5 of the TDRA's Consumer Protection Regulation v1.5 are also worded widely enough to potentially apply to electronic marketing.

The TDRA's Unsolicited Electronic Communications Regulation states that telecommunications licensees are under a general obligation to put all practical measures in place to minimise the transmission of Spam having a UAE Link across their Telecommunications Networks, and where they are aware of Spam having a UAE Link sent to or from a particular Electronic Address, they must take all practical means to end the transmission of that Spam and to prevent the future transmission of such Spam. Spam is defined as Marketing Electronic Communications sent to a Recipient without obtaining the Recipient's Consent. Although the Unsolicited Electronic Communications Regulation is targeted and enforced against telecommunications licensees, it effectively puts an obligation upon the licensees to minimise and prevent Spam from being transmitted through their networks.

Federal Decree Law No 14 of 2023 On Trading by Modern Technological Means (“**TMTM Law**”) places further obligations on merchants who trade by modern technological means to protect consumer rights when conducting business.

Article 5 of the TMTM Law places the obligation on merchants to meet the conditions and requirements approved by the competent authorities regarding the advertising and marketing campaigns and the exchange of consumer data.

Article 6 of the TMTM Law provides consumers with the right to choose whether to receive advertising and marketing campaigns or not via phone calls, emails or social media platforms.

ONLINE PRIVACY

The PDPL does not expressly cover online privacy, however the PDPL will apply to Processing online.

Although the UAE Criminal Law does not contain provisions directly relating to the internet, its provisions related to privacy are broadly drafted and therefore could apply to online matters (such as Article 432 as described above).

Additionally, as described in Collection and Processing, under certain circumstances, online privacy is protected through Articles 2, 3, 4, 6, 7, 8 and 44 of the Cyber Crime Law and the TDRA's Consumer Protection Regulation. Unlawful access via the internet, by electronic devices, of financial information (e.g. Credit Cards and Bank Accounts) without permission is a specific offence under the Cyber Crime Law (Articles 6 and 8).

The TMTM Law further provides control on the protection of consumer’s Data and Information within Article 10 of the law. Article 10(1) of the TMTM Law confirms that data protection law in the UAE shall apply to consumer information and data, its classification and ownership.

KEY CONTACTS

Eamon Holley
Special Consultant
T +971 4 438 6293
eamon.holley@dlapiper.com

Alex Mackay
Associate
T +971 4 438 6160
alex.mackay@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UGANDA

Last modified 12 January 2023

LAW

Generally, a person’s right to privacy of information is protected under Article 27 of the Constitution of the Republic of Uganda. The protection under the Constitution has recently been supplemented by the Data Protection and Privacy Act, 2019 and the Data Protection and Privacy Regulations 2021 which were enacted primarily to regulate the collection, processing, use and disclosure of personal data. The Act and Regulations apply to any person, entity or public body:

- collecting, processing, holding or using personal data within Uganda;
- outside Uganda who is collecting, processing, holding or using personal data of Ugandan citizens.

The Data Protection and Privacy Act commenced on 3 May 2019 while the Regulations took effect on 12 March 2021.

There are also other sector specific laws that incorporate data protection provisions applicable to the activities governed under those particular laws. These laws include, but are not limited to:

- The Access to Information Act, 2005
- The Regulation of Interception of Communications Act, 2010
- The Computer Misuse Act, 2011 (as amended)
- The Registration of Persons Act, 2015

DEFINITIONS

Definition of Personal Data

Personal data is defined under section 2 of the Data Protection and Privacy Act as information about a person from which the person can be identified such as information relating to nationality, age, marital status, education level, occupation and identity data.

This information is considered personal data regardless of the form in which the information is recorded.

Definition of Sensitive Personal Data

The term “*sensitive personal data*” has not been defined under Ugandan law.

However, section 9 of the Data Protection and Privacy Act defines a related term, “*special personal data*”, as data which relates to the religious or philosophical beliefs, political opinion, sexual life, financial information, health status or medical records of an individual.

NATIONAL DATA PROTECTION AUTHORITY

The Personal Data Protection Office established by Section 4 of the Data Protection and Privacy Act and Regulation 3 of the Data Protection and Privacy Regulations is responsible for personal data protection. The Office operates under the National Information Technology Authority-Uganda and was operationalized in August 2021.

REGISTRATION

Under Regulation 13 of the Data Protection and Privacy Regulations, every data collector, processor, or controller in Uganda (or outside Uganda collecting or processing the personal data of Ugandan citizens) is required to register with the Personal Data Protection Office. The Office maintains a Data Protection and Privacy Register relating to data collectors, processors and controllers, including the purpose for which the data is collected or processed.

DATA PROTECTION OFFICERS

Every entity whose activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale, or whose activities consist of processing special personal data, is required to designate a personal data protection officer charged with ensuring compliance with the data protection law. There is no criteria for appointment of the data protection officers provided by the Act or Regulations.

Under Regulation 47 of the Data Protection and Privacy Regulations, the Personal Data Protection Office is required to specify the persons, institutions, and public bodies required to designate a data protection officer. This publication is yet to be released by the Office.

COLLECTION & PROCESSING

Restrictions on the collection or processing of the personal data

There are a number of restrictions under the Data Protection and Privacy Act which ought to be complied with in the collection and processing of personal data. These include but are not limited to the following:

- The informed consent of the data subject must be obtained prior to collection or processing of personal data.
- The collection or processing of personal data relating to a child is prohibited unless: (i) done with the prior consent of the parent / guardian; (ii) necessary for compliance with the law; or (iii) the collection or processing is for research or statistical purposes.
- Special personal data should not be collected or processed unless specifically permitted by the law.
- Personal data should be collected directly from the data subject.
- Personal data shall only be collected for a lawful and specific purpose which relates to the functions or activity of the data collector or data controller.
- A data collector, data processor or data controller is obligated to ensure that the data is complete, accurate, up to-date and not misleading.
- Further processing of personal data shall only be for the specific purpose in connection with which the personal data was collected.
- Personal data shall not be retained for a period longer than is necessary to achieve the purpose for which the data is collected and processed unless specifically authorised by the Act.
- A personal data record should be destroyed or de-identified after the expiry of the retention period in a manner that prevents reconstruction of the personal data in an intelligible form.

TRANSFER

Section 19 of the Data Protection and Privacy Act permits processing or storage of personal data outside Uganda provided that:

- adequate measures are in place in the country in which the data is processed or stored which are at the least equivalent to the protection provided under the Act; or
- the data subject has consented.

Regulation 30(2) of the Data Protection and Privacy Regulations prohibits any further transfer of personal data processed outside Uganda to a third country without the consent of the data subject.

SECURITY

A data controller, data collector or data processor is required under section 20 of the Data Protection and Privacy Act to secure the integrity of personal data in its control or possession by adopting appropriate measures to prevent loss, unauthorised destruction, unauthorised processing of or unlawful access to personal data.

The data controller is specifically required to use measures that:

- identify reasonable risks to personal data in its possession or control;
- establish and maintain appropriate precautions against the risks identified;
- regularly verify the effective implementation of the precautions;
- ensure that the safeguards are continually updated.

In instances where personal data is processed by a third party, the entity must ensure that the data processor applies the security safeguards provided under the Act.

BREACH NOTIFICATION

Section 23 of the Data Protection and Privacy Act and Regulation 33 of the Data Protection and Privacy Regulations impose a duty on a data processor, data collector or data controller to immediately notify the Personal Data Protection Office, where there is reasonable belief that personal data has been accessed or acquired by an unauthorised person. Data collectors, processors and controllers registered with the Office are required to submit an annual report summarizing any data breaches suffered and how they were addressed.

ENFORCEMENT

Remedial orders

The Personal Data Protection Office is empowered under the Data Protection and Privacy Regulations to make orders requiring a breach or violation of the Act to be remedied or for compliance with a request of a data subject. The exercise of these powers may be triggered by a complaint or request lodged with the Office by a person aggrieved by actions under the Act or by a data subject seeking to enforce the rights availed under the Act.

Compensation

A person is entitled to apply to a court of law with competent jurisdiction for compensation for damage or distress caused by the actions of a data collector, data controller or data processor in violation of the Data Protection and Privacy Law.

Sanctions

- *Fines* — The Data Protection and Privacy Act provides for fines as a penalty for the commission of an offence under the Act. Save for the fine imposed on a corporation for non-compliance with Act, the fines provided do not exceed 245 currency points (which is equivalent to UGX 4,900,000). The exception in the case of a violation by a corporation allows a court to order a corporation to pay a fine of up to 2 percent of the corporation’s annual gross turnover.
- *Imprisonment* — A court of law may order imprisonment of a person convicted of any of the offences under the Data Protection and Privacy Act. The imprisonment terms which are provided are limited to a period of 10 years or less. Both imprisonment and payment of a fine can be ordered by court in respect of the same offender upon conviction of an offence.

ELECTRONIC MARKETING

There is no electronic marketing regulation in Uganda.

ONLINE PRIVACY

There is no specific online privacy regulation.

KEY CONTACTS

Sebalu & Lule Advocates
www.sebalulule.co.ug/

Barnabas Tumusingize
Managing Partner
Sebalu & Lule Advocates
T +256 213 250 013
brt@sebalulule.co.ug

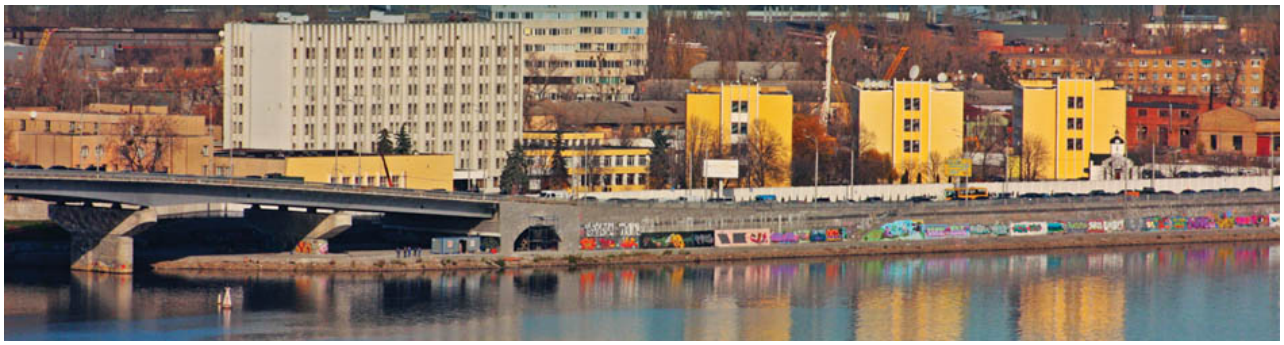
Paul Mbuga
Principal Associate
Sebalu & Lule Advocates
T +256 0312 2500013
mbuga@sebalulule.co.ug

Josephine Muhaise
Associate
Sebalu & Lule Advocates
T +256 414 233 063
jmuhaise@sebalulule.co.ug

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UKRAINE



Last modified 22 January 2024

LAW

The Law of Ukraine No. 2297 VI 'On Personal Data Protection' as of June 1, 2010 (Data Protection Law) is the main legislative act regulating personal data protection in Ukraine. On December 20, 2012, the Data Protection Law was substantially amended by the Law of Ukraine, 'On introducing amendments to the Law of Ukraine’ ’On Personal Data Protection' dated November 20, 2012, No. 5491-VI. Additional significant changes to Data Protection Law were introduced by the Law of Ukraine 'On Amendments to Certain Laws of Ukraine regarding Improvement of Personal Data Protection System' dated July 3, 2013, No. 383-VII which came into force on January 1, 2014.

In addition to the Data Protection Law, certain data protection issues are regulated by subordinate legislation specifically developed to implement the Data Protection Law, in particular:

- Procedure of notification of the Ukrainian Parliament's Commissioner for Human Rights on the processing of personal data, which is of particular risk to the rights and freedoms of personal data subjects, on the structural unit or responsible person that organizes the work related to protection of personal data during processing thereof (Notification Procedure)
- Model Procedure of processing of personal data (Model Procedure)
- Procedure of control by the Ukrainian Parliament's Commissioner for Human Rights over the adherence of personal data protection legislation

The Data Protection Law essentially complies with EU Data Protection Directive 95/46/EC.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, executed in Strasbourg on January 28, 1981 and the Additional Protocol to the Convention regarding supervisory authorities and trans-border data flows, executed in Strasbourg on November 8, 2001 were ratified by the Ukrainian Parliament on July 6, 2010 (Convention on Automatic Processing of Personal Data) and have become fully effective in Ukraine.

In addition, data protection is regulated by:

- The Constitution of Ukraine dated June 28, 1996
- The Civil Code of Ukraine dated January 16, 2003, No 435 IV
- Law of Ukraine 'On Information' No 2657 XII, dated October 2, 1992
- Law of Ukraine 'On Protection of Information in the Information and Telecommunication Systems' dated July 5, 1994 No. 80/94 VR
- Law of Ukraine ‘On Electronic Commerce’ dated September 3, 2015, No 675-VIII
- Some other legislative acts

Furthermore, on October 25, 2022 the new Draft Law “On Personal Data Protection” No. 8153 has been submitted to Ukrainian Parliament. The said draft law is aimed at harmonizing Ukrainian data protection legislation with the standards enshrined by the GDPR and Convention 108+ and is currently expecting to be considered by Ukrainian Parliament.

DEFINITIONS

Definition of personal data

Data Protection Law defines ‘personal data’ as data or an aggregation of data on an individual who is identified or can be precisely identified.

Definition of sensitive personal data

There is no definition of ‘sensitive personal data’.

However, there is general prohibition to process personal data with regard to racial or ethnic origin, political, religious ideological convictions, participation in political parties and trade unions, accusation in criminal offenses or conviction to criminal punishment, as well as data relating to the health or sex life of an individual.

Processing of such data is allowed if unambiguous consent has been given by the personal data subject or based on exemptions envisaged by Data Protection Law *(eg,* the processing is performed for the reasons of protection of vital interest of individuals, healthcare purposes, in course of criminal proceedings, anti-terrorism purposes, etc.).

NATIONAL DATA PROTECTION AUTHORITY

Starting from January 1, 2014, Ukrainian Parliament's Commissioner for Human Rights (Ombudsman) is the state authority in charge of controlling the compliance of the data protection legislation.

REGISTRATION

As of January 1, 2014, the requirement of obligatory registration of personal data databases has been abolished. However, according to new wording of Data Protection Law, personal data owners are obliged to notify the Ombudsman about personal data processing which is of particular risk to the rights and freedoms of personal data subjects within 30 working days from commencement of such processing. Pursuant to the Notification Procedure, the following types of personal data processing requires obligatory notification to the Ombudsman:

- Racial, ethnic, national origin
- Political, religious ideological beliefs
- Participation in political parties and/or organizations, trade unions, religious organizations or civic organization of ideological direction
- State of health
- Sexual life
- Biometric data
- Genetic data
- Criminal or administrative liability
- Application of measures as part of pre-trial investigation
- Any investigative procedures relating to an individual
- Acts of certain types of violence used against an individual
- Location and / or route of an individual

The Notification Procedure envisages that the application for notification shall contain, inter alia the following information:

- Information about the owner of personal data
- Information about the processor(s) of personal data
- Information on the composition of personal data being processed
- The purpose of personal data processing
- Category(ies) of individuals whose personal data are being processed
- Information on third parties to whom the personal data are transferred
- Information on cross-border transfers of personal data

- Information on the place (address) of processing of personal data
- General description of technical and organizational measures taken by personal data owner in order to maintain the security of personal data

Where any of information listed above is submitted to the Ombudsman and has changed, the owner of the personal data shall notify the Ombudsman on such changes within 10 days from the occurrence of such change.

Additionally, the Notification Procedure requires the owners of personal data to notify the Ombudsman regarding the termination of personal data processing which is of particular risk to the rights and freedoms of personal data subjects, within ten days of such termination.

The Notification Procedure requires owners and processors of personal data that process personal data, which is of particular risk to the rights and freedoms of personal data subjects, to notify the Ombudsman on establishing a structural unit or appointing a person (data protection officer) responsible for the organization of work related to the protection of personal data during the processing. Such notification shall be made within 30 days of establishing a structural unit or appointing a responsible person.

Information regarding the said notifications of the Ombudsman shall be published on the official website of the Ombudsman.

DATA PROTECTION OFFICERS

Data owners and processors processing personal data that is of particular risk to the rights and freedoms of personal data subjects, must establish a special department or appoint a responsible person (data protection officer) to be responsible for the personal data processing matters. Other owners and processors may either establish a department or appoint a responsible person on a voluntary basis.

There are no requirements for the data protection officer to be a citizen or a resident in Ukraine. However, if he or she is a foreign citizen under the general rule, a work permit must be obtained for him or her to hold such a position. There are no particular penalties for the incorrect appointment of Data Protection Officer.

COLLECTION & PROCESSING

The Data Protection Law requires obtaining the consent of data subjects for the processing of their personal data. According to the Data Protection Law, the consent of the data subject means the voluntary and intentional expression of will of the data subject to the processing of personal data for the identified purposes, expressed in writing or in some other form. In the area of e-commerce, consent may be granted in the process of registration of data subjects by "ticking" a consent box during registration, provided that such a system does not allow processing of personal data before the consent is obtained. Under certain circumstances, personal data may be processed without a data subject’s consent (*eg*, legislative permission for processing of personal data, necessary to the conclusion and execution of a transaction or contract in favor of the data subject, protection of interests of data subject or data owner).

Pursuant to the Data Protection Law, as a general rule, personal data subjects shall be informed, at the moment of collection of their personal data of:

- The owner of their personal data
- The composition and content of their personal data being collected
- Their rights
- The purpose of their personal data collection, and
- The persons to whom their personal data will be transferred

However, in cases when the personal data of individuals have been collected based on the following grounds, the personal data subjects shall be informed of the above within 30 working days from the:

- Legislative permission of the owner of the personal data on the processing of personal data exclusively for the purposes of fulfilling its authorities

- Conclusion and execution of a transaction where the data subject is a party or the transaction has been concluded in favor of the data subject, which preceded conclusion of a transaction at the request of the subject of personal data
- Protection of vital interests of the data subject, or
- Need to protect the legitimate interests of the owner of personal data and third parties, except where a data subject requests that the processing of his/her personal data stops and the need to protect personal data prevails over such interest

In addition, the Data Protection Law provides the data subject with the following rights:

- To be aware of the sources of collection, location of his / her personal data, the purpose of data processing, the address of the owner or processor of the personal data or to obtain the said information through his / her representatives
- To obtain information in regards to the conditions of providing access to personal data, and in particular, information on third parties, to which his / her personal data are transferred
- To access his / her personal data
- To obtain a reply within 30 calendar days from the date of the receipt of his / her request, informing the individual whether his / her personal data is being processed and to receive the contents of such personal data
- To provide the owner of personal data with the reasonable request to terminate the processing of his / her personal data
- To provide a reasonable request to change or destroy his / her personal data by any owner and processor of the personal data if the data is processed illegally or is inaccurate
- To protect of his / her personal data from unauthorized processing and accidental loss, elimination or damage with respect to intended encapsulation, not providing or the untimely provision of personal data, and to protect from providing invalid or discrediting information regarding the individual
- To appeal violations in the course of personal data processing to the Ombudsman or to the court
- To introduce limitations as regards rights on its personal data processing while giving the consent
- To use the means of legal protection in the case of violation of rights to personal data
- To revoke its consent on personal data processing
- To be aware of the mechanism of automatic personal data processing, and
- To be protected from the automated decision that has legal effects

The owner of the personal data can entrust the processing of personal data to the processor pursuant to a written agreement requiring that the processor process the personal data only for the purposes and in the amount permitted under the agreement. The transfer of personal data to the processor is permitted only with consent of the data subject.

TRANSFER

In accordance with Data Protection Law, personal data may be transferred to foreign parties when there is an appropriate level of protection of personal data in the respective state of the transferee. Pursuant to the Data Protection Law, such states include member states of the European Economic Area and signatories to the EC Convention on Automatic Processing of Personal Data. The list of the states ensuring an appropriate level of protection of personal data will be determined by the Cabinet of Ministers of Ukraine.

Personal data may be transferred abroad based on one of the following grounds:

- Unambiguous consent of the personal data subject
- Cross-border transfer is needed to enter into or perform a contract between the personal data owner and a third party in favor of the data subject
- Necessity to protect the vital interests of the data subject
- Necessity to protect public interest, establishing, fulfilling and enforcing of a legal requirement
- Non-interference in personal and family life of the data subject, as guaranteed by the data owner

SECURITY

The data owners and processors must take appropriate technical and organizational measures to ensure the protection of personal data against unlawful processing, including against loss, unlawful or accidental elimination, and also against unauthorized

access. In this regard, owners and processors processing personal data which is of particular risk to the rights and freedoms of personal data subjects shall determine a special department or a responsible person to organize the work related to the protection of personal data during the processing thereof (other owners and processors may either establish a department or appoint a responsible person on a voluntary basis).

The Model Procedure stipulates that the owners and processors of personal data shall take measures to maintain the security of personal data in all stages of their processing, including organizational and technical measures for the protection of personal data. Organizational measures shall include:

- Determination of a procedure of access to personal data by employees of the owner / processor of personal data
- Determination of the order of the recording of operations related to the processing of personal data o and access to them
- Elaboration of an action plan in case of unauthorized access to personal data, damage of technical equipment or occurrence of emergency situations, and
- Regular trainings of employees working with personal data

Personal data, irrespective of the manner of its storage, shall be processed in the way which makes unauthorized access to the data by third persons impossible.

With the purpose of maintenance of security of personal data, technical security measures shall be taken which would exclude the possibility of unauthorized access to personal data being processed and ensure the proper work of technical and program complex through which the processing of personal data is performed.

Additionally, the Data Protection Law requires establishing a structural unit or appointing a responsible person within the personal data owners / processors processing the personal data which is of particular risk to the rights and freedoms of personal data subjects. Such structural unit or responsible person shall organize the work related to protection of personal data during the processing thereof.

BREACH NOTIFICATION

There is no requirement to report data security breaches or losses to the appropriate state authority.

ENFORCEMENT

According to Data Protection Law, the Ombudsman and Ukrainian courts are responsible for overseeing the compliance of personal data protection legislation. Failure to comply with the provisions of Data Protection Law can lead to the penalties prescribed by the law.

Violation of personal data protection legislation may result in civil, criminal and administrative liability.

If the violation has led to material or moral damages, the violator may be required by the court to reimburse such damages.

The Code of Ukraine on Administrative Offenses envisages administrative liability for the following breaches of Ukrainian data protection legislation:

- Failure to notify or delay in providing notification to the Ombudsman regarding the processing of personal data or of a change to the information submitted, subject to notification requirements under Ukrainian legislation, or submission of incomplete or false information, which may lead to a fine of up to EUR 164;
- Non-fulfilment of legitimate requests (orders) from the Ombudsman or determined state officials of the Ombudsman's secretariat, regarding the elimination or prevention of violations of personal data protection legislation, which may lead to a fine of up to EUR 411;
- Non-observance of the established procedure for the protection of personal data which leads to the unauthorized access of the personal data or violation of rights of the data subject, which may lead to a fine of up to EUR 411.

The criminal liability, prescribed by the Criminal Code of Ukraine, envisages fines of up to EUR 411 or correctional works for a term of up to two years, up to six months arrest, or up to three years of limitation of freedom for the illegal collection, storing, use, elimination, or spreading of confidential information about an individual, or an illegal change of such information.

ELECTRONIC MARKETING

The Law of Ukraine ’On Electronic Commerce’ dated September 3, 2015 provides for certain legal requirements for distribution of commercial electronic messages in the area of electronic commerce (i.e. electronic messages in any form, the purpose of which is to promote, directly or indirectly, goods, works, services, business reputation of a party engaged in a business or self-employed professional activity). In particular, commercial electronic messages shall be distributed only subject to the consent given by individual to whom such messages are addressed. At the same time, commercial electronic messages may be distributed to an individual without his / her consent only if such individual has an option to object to receiving such messages in future.

In addition, commercial electronic messages shall satisfy the following criteria:

- Commercial electronic messages shall unequivocally be identified as such.
- The recipient shall have easy access to information regarding the person sending the message as stipulated by the Law of Ukraine ‘On Electronic Commerce’, in particular:
    - full name of legal entity / individual and place of registration / residence;
    - email / website of the online shop;
    - registration number or tax ID number / passport details (for individuals);
    - license data (in case if it is mandatory under the law);
    - inclusion of taxes in calculation of the price of goods / services; and
    - price of delivery of goods (in case if delivery is performed).
- Commercial electronic messages regarding sales, promotional gifts, premiums and etc. shall be unequivocally identified as such and the conditions of receiving of such promotions shall be clearly stated to avoid their ambiguous understanding as well as shall comply with advertising legislation.

In addition, under the Law of Ukraine "On Electronic Communications" dated December 16, 2020, end-users may use telephone numbers or other network subscriber identifiers obtained by any person in the course of selling goods or providing services to send advertisements for the purpose of selling goods or services only with the consent of the end-user, including in electronic form, and if the recipient is given the opportunity to refuse the use of his or her data at any time, free of charge, in a simple and understandable manner.

Furthermore, distribution of spam is generally prohibited. Spam is defined quite broadly as more than five messages (electronic, text and / or multimedia messages) sent to one recipient without the recipient's prior consent.

ONLINE PRIVACY

There is no specific legislation regulating online privacy in Ukraine. However, the Data Protection Law applies to the extent online activities involve the processing of personal data.

KEY CONTACTS

Natalia Kirichenko
Partner
Kinstellar Ukraine LLC
T +380 (44) 490 9575

natalia.kirichenko@kinstellar.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UNITED KINGDOM

Last modified 22 January 2024

LAW

Following the UK’s exit from the European Union, the UK Government has transposed the General Data Protection Regulation (Regulation (EU) 2016/679) into UK national law (thereby creating the **“UK GDPR”**). In so doing, the UK has made a number of technical changes to the GDPR in order account for its status as a national law of the United Kingdom (e.g. to change references to **“Member State”** to **“the United Kingdom”**). These changes were made under the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. *At this time, all material obligations on controller and processors essentially remain the same under the UK GDPR as under the ‘EU GDPR’.*

The Data Protection Act 2018 (**“DPA”**) remains in place as a national data protection law, and supplements the UK GDPR regime. It deals with matters that were previously permitted derogations and exemptions from the EU GDPR (for example, substantial public interest bases for the processing of special category data, and context-specific exemptions from parts of the GDPR such as data subject rights).

In addition,

- Part 3 of the DPA transposes the Law Enforcement Directive ((EU) 2016/680) into UK law, creating a data protection regime specifically for law enforcement personal data processing;
- Part 4 of the DPA updates the data protection regime for national security processing; and
- Parts 5 and 6 set out the scope of the Information Commissioner's mandate and her enforcement powers, and creates a number of criminal offences relating to personal data processing.

On 8 March 2023, the new ‘Data Protection and Digital Information (No. 2) Bill’ (“the Bill”) was introduced to Parliament following on from the consultation by the Department for Culture, Media and Sport on data protection reforms. The anticipated reforms aim to reduce the compliance burden on organisations. A few of the proposed changes in the Bill include:

- Amendments to certain definitions, such as “identifiable living individual” (impacting the definition of “personal data”) and the meaning of research and statistical purposes;
- Amendments to data protection principles, including the addition of recognised ‘legitimate interests’ to assist with determining an applicable legal basis;
- Amendments to the conduct of data subject rights, by recognising requests that may be “vexatious or excessive”; and
- Amendments to the obligations of controllers and processors which generally provide more flexibility than the current position, for example with regard to complying with accountability obligations.

It is expected that the Bill will be debated and amended further as it passes through the House of Lords in the first months of 2024, and will likely be enacted through the course of the year.

Territorial Scope

The application of the UK GDPR turns principally on whether an organization is established in the United Kingdom. As under the EU GDPR, an 'establishment' may take a wide variety of forms, and is not limited to a company registered in the United Kingdom.

The UK GDPR also has extra-territorial effect, following the same principles as set out in the EU GDPR. As a result, an organisation that it is not established within the United Kingdom will be subject to the UK GDPR if it processes personal data of data subjects who are in the United Kingdom where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) to such data subjects in the United Kingdom or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the United Kingdom.

DEFINITIONS

"Personal data" is defined as "any information relating to an identified or identifiable natural person" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “all means reasonably likely to be used” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The UK GDPR creates more restrictive rules for the processing of "special categories" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to criminal convictions and offences (Article 10).

The UK GDPR is concerned with the "processing" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "controller" or a "processor". The controller is the decision maker, the person who "alone or jointly with others, determines the purposes and means of the processing of personal data" (Article 4). The processor "processes personal data on behalf of the controller", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "data subject" is a living, natural person whose personal data are processed by either a controller or a processor.

"Public authority" and "public body" are expressions used in the UK GDPR. The DPA defines them by reference to the definition of "public authority" used in the Freedom of Information Act 2000.

The DPA also clarifies that, where the purpose and means of processing are determined by an enactment of law, then the person on whom the obligation to process the data is imposed by the enactment is the controller.

NATIONAL DATA PROTECTION AUTHORITY

The Information Commissioner (whose functions are discharged through the Information Commissioner's Office **("ICO")**) is the supervisory authority for the UK for the purposes of Article 51 of the UK GDPR. Following Brexit, the ICO no longer has influence or membership in the European Data Protection Board and can no longer be nominated as a lead supervisory authority under the EU GDPR regime. This is reflected in the UK GDPR which omits Chapter 7 (Cooperation and Consistency) of the EU GDPR, on the basis that the UK will not be part of the EU’s cooperation and consistency mechanisms.

The ICO's contact details are:

Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

T +0303 123 1113 (or +44 1625 545745 if calling from overseas)

F 01625 524510

www.ico.org.uk

REGISTRATION

The UK operates a fee-paying scheme for controllers under the Data Protection (Charges and Information) Regulations 2018, known as the ‘Data Protection Fee’. All controllers have to pay the data protection fee to the ICO annually, unless they are exempt from doing so.

The UK Government has set the fee tiers based on its perception of the risks posed by controllers processing personal data. The amount payable depends upon staff numbers and annual turnover or whether the controller is a public authority, a charity or a small occupational pension scheme. Not every controller must pay a fee – there are exemptions. The maximum fee, for large organisations, is GBP 2,900.

The maximum penalty for a controller who breaks the law by not paying a fee (or not paying the correct fee) is a fine of GBP 4,350 (150% of the top tier fee).

DATA PROTECTION OFFICERS

Under the UK GDPR, each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "expert knowledge" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "properly and in a timely manner in all issues which relate to the protection of personal data" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in the UK GDPR, include (Article 39):

- to inform and advise on compliance with the UK GDPR and other UK data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the UK GDPR. Organisations must not only comply with the UK GDPR but also be able to demonstrate compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6 (1)):

- with the consent of the data subject (where consent must be "freely given, specific, informed and unambiguous", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (under UK law) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Categories of Personal Data

Processing of special categories of personal data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of United Kingdom law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;

- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Schedule 1 to the DPA supplements the requirements for processing special categories of personal data, and also provides for a number of ‘substantial public interest’ grounds that can be relied upon to process special categories of personal data in specific contexts which are deemed to be in the public interest. Many of these grounds are familiar from the previous UK law, whilst other are new. Important examples include:

- processing required for employment law;
- heath and social care;
- equal opportunity monitoring;
- public interest journalism;
- fraud prevention;
- preventing / detecting unlawful acts (eg money laundering / terrorist financing);
- insurance; and
- occupational pensions.

Criminal convictions and offences data (Article 10)

The processing of criminal conviction or offences data is prohibited by Article 10 of the UK GDPR, except where specifically authorised under relevant member state law. Part 3 of Schedule 1 of the DPA authorises a controller to process criminal conviction or offences data where the processing is necessary for a purpose which meets one of the conditions in Parts 2 of Schedule 1 (this covers the conditions noted above other than processing for employment law, health and social care), as well as number of other specific conditions:

- consent;
- the protection of a data subject's vital interests; and
- the establishment, exercising or defence of legal rights, the obtaining of legal advice and the conduct of legal proceedings

Appropriate policy and additional safeguards

In any case where a controller wishes to rely on one of the DPA conditions to lawfully process special category, criminal conviction or offences data, the DPA imposes a separate requirement to have an appropriate policy document in place and apply additional safeguards to justify the processing activity. The purpose of the policy document is to set out how the controller intends to comply with each of the data protection principles in Article 5 of the UK GDPR in relation to this more sensitive processing data activity.

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The UK GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation.

Transparency (Privacy Notices)

The UK GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of UK GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data replicating those in the EU GDPR. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "which produces legal effects concerning [the data subject] … or similarly significantly affects him or her" is only permitted where:

- necessary for entering into or performing a contract;
- authorised by UK law; or
- the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view. Further safeguards for automated decisions that are necessary for entering into or performing a contract or which are authorised by UK law are set out in section 14 of the DPA.

Child's consent to information society services (Article 8)

Article 8(1) of the UK GDPR stipulates that a child may only provide their own consent to processing in respect of information society (primarily, online) services, where that child is over 16 years of age, unless UK law applies a lower age. The DPA reduces the age of consent for these purposes to 13 years for the UK.

TRANSFER

Transfers from the UK

Transfers of personal data by a controller or a processor to third countries outside of the United Kingdom are only permitted where the conditions laid down in the UK GDPR are met (Article 44).

The United Kingdom Government has the power to make an adequacy decision in respect of a third country under the UK GDPR (Article 45). This power is equivalent to the similar authorities granted to the EC has under the EU GDPR and involves the Secretary of State making a positive determination that the third country provides for adequate level of data protection, following which personal data may be freely transferred to that third country (Article 45(1)). On 21 September 2023, the United Kingdom Government adopted its adequacy decision for the UK Extension for the EU-US Data Privacy Framework, in which an adequate level of protection for personal data transferred the UK to US companies that have joined the framework is ensured in accordance with UK GDPR Art. 45. Currently, the following countries or territories enjoy UK adequacy decisions (these have all essentially been 'rolled over', on a temporary basis, from the EU GDPR): Andorra, Argentina, Canada (with some exceptions),

Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, Eastern Republic of Uruguay, United States (if certified under the UK Extension to the EU-US Data Privacy Framework) and New Zealand. The UK is also treating all EU and EEA Member States as adequate jurisdictions, again on a temporary basis. The United Kingdom intends to reassess all these adequacy decisions before the end of 2024. It also has the power to make its own adequacy decisions, and likely time consider new candidates for UK adequacy.

Transfers to third countries are also permitted where **appropriate safeguards** have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available (Article 46). The list of appropriate safeguards includes, amongst others, binding corporate rules and standard contractual clauses with additional safeguards to guarantee an essentially equivalent level of protection to data subject’s and their personal data[1].

Schedule 21 to the DPA provides that the EU Commission approved standard contractual clauses may continue to be used for transfers under the UK GDPR, until such time as they replaced by clauses issued by the UK Government. Note that the standard contractual clauses carried into UK law are those which were in use as at the end of 2020. It is expected these will be updated during the course of 2021.

Article 49 of the UK GDPR also includes a list of context specific **derogations**, permitting transfers to third countries where:

- explicit informed consent has been obtained;
- the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
- the transfer is made from a register which according to domestic law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the United Kingdom (Article 48) are only recognised or enforceable (within the United Kingdom) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the United Kingdom; a transfer in response to such requests where there is no other legal basis for transfer will infringe the UK GDPR.

Transfers from the EU to the UK

The UK is now a third country for the purposes of Chapter V of the EU GDPR. .

On 28 June 2021, the EU adopted adequacy decisions in relation to the UK, recognising that the UK offers an equivalent level of protection of personal data as compared to the EU. This therefore enables personal data to flow freely from the EU to the UK.

For more information, please visit our Transfer - global data transfer methodology website.

1. Following the decision of the Court of Justice of the European Union in the *Data Protection Commissioner v. Facebook and Max Schrems* case (the ‘Schrems II’ case)

SECURITY

The UK GDPR is not prescriptive about specific technical standards or measures. Rather, the UK GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the UK GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

BREACH NOTIFICATION

The UK GDPR contains a general requirement for a personal data breach to be notified by the controller to the ICO, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the ICO without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the ICO must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the ICO.

Breaches in the United Kingdom can be reported to the ICO's dedicated breach helpline during office hours (+44 303 123 1113). Outside of these hours (or where a written notification is preferred) a pro forma may be downloaded and emailed to the ICO.

ENFORCEMENT

Fines

The UK GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or GBP 17.5 million (whichever is higher).

It is the intention that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the UK GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to GBP 17.5 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by domestic law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to GBP 8.7 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

The ICO is not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions. To date, the ICO has issued several fines under GDPR, ranging from GBP 275,000 to GBP 20 million.

Investigative and corrective powers

The ICO also enjoys wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The UK GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the UK GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with the ICO (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of the ICO concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The DPA sets out the specific enforcement powers provided to the ICO pursuant to Article 58 of the UK GDPR, including:

- information notices – requiring the controller or processor to provide the ICO with information;
- assessment notices – permitting the ICO to carry out an assessment of compliance;
- enforcement notices – requiring the controller or processor to take, or refrain from taking, certain steps; and
- penalty notices – administrative fines.

The ICO has the power to conduct a consensual audit of a controller or a processor, to assess whether that organisation is complying with good practice in respect of its processing of personal data.

Under Schedule 15 of the DPA, the ICO also has powers of entry and inspection. These will be exercised pursuant to judicial warrant and will allow the ICO to enter premises and seize materials.

The DPA creates two new criminal offences in UK law: the re-identification of de-identified personal data without the consent of the controller and the alteration of personal data to prevent disclosure following a subject access request under Article 15 of the GDPR. The DPA retains existing UK criminal law offences, eg offence of unlawfully obtaining personal data.

The DPA requires the ICO to issue guidance on its approach to enforcement, including guidance about the circumstances in which it would consider it appropriate to issue a penalty notice, i.e. administrative fine.

The DPA also requires the ICO to publish statutory codes of practice on direct marketing and data sharing (preserving the position under the previous law).

ELECTRONIC MARKETING

The UK GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the UK GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are found in the Privacy and Electronic Communications Regulations 2003 (as amended) (**“PEC Regulations”**). The PEC Regulations are derived from European Union Directive 2002/58/EC (ePrivacy Directive), which have been retained in UK law post-Brexit.

The PEC Regulations prohibit the use of automated calling systems without the consent of the recipient. The PEC Regulations also prohibit unsolicited electronic communications (ie by email or SMS text) for direct marketing purposes without prior consent from the consumer unless:

- the consumer has provided their relevant contact details in the course of purchasing a product or service from the person proposing to undertake the marketing
- the marketing relates to offering a similar product or service, and
- the consumer was given a means to readily 'opt out' of use for direct marketing purposes both at the original point where their details were collected and in each subsequent marketing communication.

Each direct marketing communication must not disguise or conceal the identity of the sender and include the 'unsubscribe' feature referred to above.

The restrictions on marketing by email / SMS only applies in relation to individuals and not where marketing to corporate subscribers.

Enforcement of a breach of the PEC Regulations is dealt with by the ICO. The maximum fine for a breach of the PEC Regulations is GBP 500,000, which can be issued against a company or its directors. The ICO regularly issues fines for direct marketing violations, and it is not uncommon for these to be in the hundreds of thousands of pounds range.

ONLINE PRIVACY

The PEC Regulations (as amended) deal with the collection of location and traffic data by public electronic communications services providers (**"CSPs"**) and use of cookies (and similar technologies).

Traffic Data

Traffic Data held by a CSP must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication.

However, Traffic Data can be retained if:

- it is being used to provide a value added service, and
- consent has been given for the retention of the Traffic Data.

Traffic Data can also be processed by a CSP to the extent necessary for:

- the management of billing or traffic
- dealing with customer enquiries
- the prevention of fraud, or
- the provision of a value added service.

Cookie Compliance

The use and storage of cookies and similar technologies requires:

- clear and comprehensive information, and
- consent of the website user.

The ICO released comprehensive guidance on the use of cookies and similar technologies in 2019. In line with the standard for ‘GDPR like’ consent under the PEC Regulations, this guidance significantly raised the bar in terms of the ICO’s expectations for cookie consent collection. It is now clear that the ICO expects consent to be collected on a clear opt-in basis – implied consent (such as the continued browsing of a website after being shown a cookie banner) is no longer sufficient. Instead, cookie consent modules that given users granular choices about cookie selection (typically on a ‘ by purpose’ basis) are becoming the norm in order to align with the guidance.

Consent is not required for cookies that are:

- used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or
- strictly necessary for the provision of a service requested by the user.

Enforcement of a breach of the PEC Regulations is dealt with by the ICO. The maximum fine for a breach of the PEC Regulations is GBP 500,000, which can be issued against a company or its directors.

KEY CONTACTS

Andrew Dyson
Partner, Global Co-Chair Data Protection, Privacy and Security Group
T +44 (0)113 369 2403
andrew.dyson@dlapiper.com

Ross McKean
Partner
T +44 (0) 20 7796 6077
ross.mckean@dlapiper.com

James Clark
Partner
T +44 113 369 2461
james.clark@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UNITED STATES

Last modified 29 January 2023

LAW

United States privacy law is a complex patchwork of national, state and local privacy laws and regulations. There is no comprehensive national privacy law in the United States. However, the US does have a number of largely sector-specific privacy and data security laws at the federal level, as well as many more privacy laws at the state (and local) level. In recent years, beginning with California, states have begun to introduce their own comprehensive privacy laws, and other states are expected to follow and enact their own comprehensive state privacy laws. Although a bipartisan draft bill (the ‘American Data Privacy and Protection Act’) was introduced in 2022, several senators were in opposition of the bill, and comprehensive privacy law on the federal level is not expected to pass any time soon.

Federal and State Privacy Laws and Regulations

Federal laws and regulations include those that apply to financial institutions, telecommunications companies, credit reporting agencies and healthcare providers, as well as driving records, children’s privacy, telemarketing, email marketing and communications privacy laws.

There are also a number of state privacy and data security laws that overlap with federal law—some of these state laws are preempted in part by federal laws, but others are not. US states have also passed privacy and data security laws and regulations that apply across sectors and go beyond federal law—such as data security laws, secure destruction, Social Security number privacy, online privacy, biometric information privacy, and data breach notification laws. Generally, each state’s laws apply to personal information about residents of that state or activities that occur within that state. Thus, many businesses operating in the United States must comply not only with applicable federal law, but also with numerous state privacy and security laws and regulations.

For example, California alone has more than 25 state privacy and data security laws, including the California Consumer Privacy Act (CCPA) and its regulations as recently amended by the California Privacy Rights Act (CPRA), collectively referred to as the CCPA. The CCPA, as amended, introduced additional definitions and individual rights, and imposed additional requirements and restrictions on the collection, use and disclosure of personal information. The CCPA is also unique among state comprehensive privacy laws in that, as of January 1, 2023, it applies to HR and B2B personal information. Enforcement of the CPRA amendments to the CCPA commenced on July 1, 2023 for violations of the new provisions that occur on or after that date.

Notably, updated CCPA regulations based on the CPRA amendments were finalized on March 29, 2023, with enforcement by the California Attorney General and the newly established California Privacy Protection Agency (‘CPPA’ or ’Agency’) expected to begin on July 1, 2023. However, following a suit filed by the California Chamber of Commerce, the Sacramento district court ruled that the Agency was required to give businesses 12-months between finalizing a CCPA regulation and commencing enforcement, effectively delaying enforcement of the amended regulations to March 29, 2024. This delay does not affect the Agency or the California Attorney General’s ability to enforce the version of the CCPA amended by the CPRA (effective July 1, 2023) or the existing (i.e., pre-2023-amendment) CCPA regulations (effective August 14, 2020).

In late 2022, the California legislature also passed the California Age-Appropriate Design Code, which was slated to take effect July 1, 2024 and would apply to companies that meet the definition of “business” under the CCPA and that provide online services that are likely to be accessed by individuals under 18 years of age. However, on September 18, 2023, a California District Court issued an injunction blocking the law from coming into effect on First Amendment grounds. Following an appeal to the Ninth Circuit by the California Attorney General's office, the fate of the law is currently uncertain. More information on the California Age-Appropriate Design Code can is available at https://www.dlapiper.com/en-us/insights/publications/2023/05/californias-age-appropriate-design-code-act

Beyond California, Colorado's Attorney General finalized the Colorado Privacy Act (CPA) Rules on March 15, 2023, which add significantly to the CPA’s obligations on businesses. Both the CPA and the CPA Rules went into effect July 1, 2023. Connecticut, Utah, and Virginia’s privacy laws also took effect in 2023.

While not identical, the Colorado, Connecticut, Utah, and Virginia state privacy laws are substantially similar to each other in most key aspects. Further, unlike the CCPA, all are also generally inapplicable to personal information collected about, and processed in the context of, employee and business relationships. On the other hand, while the CCPA has some practical similarities with these state laws, it adopts more granular definitions, requirements, and restrictions that vary considerably from these laws, and, notably, applies to personal information collected from California residents in employment and B2B contexts.

2023 brought a significant development in the health data space, with Washington passing the My Health My Data Act (MHMD). The law ostensibly applies only to consumer health data, but its exceptionally broad definitions and scope combined with its private right of action may mean its enforcement touches on data many companies may not typically consider “health” data. More information on the MHMD Act is available at https://www.dlapiper.com/en/insights/publications/2023/04/washington-state-passes-my-health-my-data-act

Finally, the pace of state privacy legislation accelerated in 2023 overall, with the following states passing their own comprehensive privacy laws or variations thereof:

- Florida (effective July 1, 2024)
- Oregon (effective July 1, 2024)
- Texas (effective July 1, 2024)
- Montana (effective Oct. 1, 2024)
- Delaware (effective Jan. 1, 2025)
- Iowa (effective Jan. 1, 2025)
- Tennessee (effective Jan. 1, 2025)
- New Jersey (effective Jan. 15, 2025)
- Indiana (effective Jan. 1, 2026)

More information on the US state privacy laws is available at https://privacymatters.dlapiper.com/state-privacy-laws/

Enforcement of Unfair and Deceptive Trade Practices

In the United States, consumer protection laws, which prohibit unfair and deceptive business practices, provide another avenue for enforcement against businesses for their privacy and security practices.

At the federal level, the US Federal Trade Commission (FTC) uses its authority to protect consumers against unfair or deceptive trade practices, to take enforcement actions against businesses for materially unfair privacy and data security practices. The FTC uses this authority to, among other things, take enforcement actions and investigate companies for:

- Failing to implement reasonable data security measures
- Making materially inaccurate or misleading privacy and security statements, including in privacy policies
- Failing to abide by applicable industry self-regulatory principles
- Transferring or attempting to transfer personal information to an acquiring entity in a bankruptcy or M&A transaction, in a manner not expressly disclosed on the applicable consumer privacy policy

- Violating consumer privacy rights by collecting, using, sharing or failing to adequately protect consumer information, in violation of standards established in their prior enforcement precedents

Many state attorneys general have similar enforcement authority over unfair and deceptive business practices, including failure to implement reasonable security measures and violations of consumer privacy rights that harm consumers in their states. State attorneys general also sometimes work together on enforcement actions against companies for actions that broadly affect the consumers of multiple states (such as data breaches).

Privacy class actions also continue to be a key risk area in the United States, including in the context of biometric privacy (under the Illinois Biometric Privacy Act), text messaging (under the federal Telephone Consumer Privacy Act) and call recording, wiretapping and related claims under the California Invasion of Privacy Act and other state laws. Online monitoring and targeting activities—including via cookies, pixels, chat bots, and so-called “session replay” tools—are an area of particular focus in the United States from a regulator and enforcement perspective and are also a developing litigation risk area.

DEFINITIONS

Definition of personal data

Varies widely by law and regulation. The definition of personal information varies under US law. Some laws—such as data breach and security laws—apply more narrowly, to sensitive personal information, such as government identifiers, financial account information, password, biometrics, health insurance or medical information, and other information that can lead to identity fraud and theft or financial harm. On the other hand, under a number of state and federal laws, personal information broadly includes any information that identifies or is linked or reasonably linkable to an individual.

California

Under the CCPA, personal information includes information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The definition specifically includes name, alias, contact information, government IDs, biometrics, genetic data, location data, account numbers, education history, purchase history, online and device IDs, and search and browsing history and other online activities, if such information is linked or linkable with a particular consumer or household. Excluded from the definition are deidentified information and information lawfully made publicly available through various means, such as through government records or by the consumer.

Under the law, 'consumer' is broadly defined as any resident of California.

Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, New Jersey, Oregon, Tennessee, Texas, Utah, Virginia

Under the other thirteen comprehensive state privacy laws, personal data includes information that is linked or reasonably linkable to an identified or identifiable individual, who is a resident of the particular state acting an individual or household capacity. Deidentified data, personal data made publicly available, and personal data about individuals acting in an employment or B2B context are generally not in scope.

Definition of sensitive personal data

Varies widely by sector and by type of statute.

Generally, includes personal health data, financial data, credit worthiness data, student data, biometric data, personal information collected online from children under 13, and information that can be used to carry out identity theft or fraud are considered sensitive, and subject to additional restrictions and regulations.

For example, state breach notification laws and data security laws generally apply to more sensitive categories of information, such as Social security numbers and other government identifiers, credit card and financial account numbers, passwords and user credentials, health or medical information, insurance ID, digital signatures, and/or biometrics.

California

The CCPA defines *sensitive personal information* as personal information that reveals about a consumer one or more of the following types of information, including:

- Social Security, driver’s license, state identification card or passport number
- account log-in, financial account, debit card or credit card number in combination with any required security or access code, password or credentials allowing access to an account
- precise geolocation
- racial or origin, citizenship or immigration status, religious or philosophical beliefs, or union membership
- contents of a consumer’s mail, email, and text messages unless the business is the intended recipient of the communication
- genetic data
- biometric information
- health information
- information about sex life or sexual orientation

Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, New Jersey, Oregon, Tennessee, Texas, Utah, Virginia

Under the other thirteen comprehensive state privacy laws, the definition of *sensitive data* is a sub-cateogry of peronsal data and largely the same with various states adding or subtracting certain data elements from the above list.

Washington

Washington’s MHMD Act introduced a very broad definition of *consumer health data*, which includes: “personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status."

For the purposes of this definition, physical or mental health status includes, but is not limited to:

- Individual health conditions, treatment, diseases, or diagnosis
- Social, psychological, behavioral, and medical interventions
- Health-related surgeries or procedures
- Use or purchase of prescribed medication
- Bodily functions, vital signs, symptoms, or measurements of the information described in subsection (8)(b)
- Diagnoses or diagnostic testing, treatment, or medication
- Gender-affirming care information
- Reproductive or sexual health information
- Biometric data
- Genetic data
- Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies
- Data that identifies a consumer seeking health care services
- Any information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with the data described in (b)(i) through (xii) of this subsection that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning)

This definition could arguably include any category of personal data (e.g., the inclusion of inference data makes it difficult to exclude any data whatsoever in the health, wellness, and fitness space). In addition, “health care services” includes any service provided to a person to assess, measure, improve, or learn about a person's health.

NATIONAL DATA PROTECTION AUTHORITY

There is no single national authority.

With some exceptions (such as for banks, credit unions and insurance companies), the FTC has jurisdiction over most commercial entities and has authority to issue and enforce federal privacy regulations (including telemarketing, email marketing, and children's privacy) and to take enforcement action to protect consumers against unfair or deceptive trade practices, including materially unfair privacy and data security practices.

Many state attorneys general have similar enforcement authority over unfair and deceptive business practices, including failure to implement reasonable security measures and violations of consumer privacy rights that harm consumers in their states.

California

The California Attorney General and the California Privacy Protection Agency (the Agency) share authority to enforce the CCPA.

California consumers also have a private right of action under the CCPA for certain data breaches, and the CCPA provides for statutory damages.

Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, New Jersey, Oregon, Tennessee, Texas, Utah, Virginia

State Attorneys General in all the other thirteen states have authority to enforce their state comprehensive privacy laws. Additionally, in some states such as Colorado, district attorneys can enforce the law.

None of these states currently provide for a private right of action.

Washington

The Washington Attorney General has the authority to enforce the MHMD Act.

Washington residents also have a private right of action under the Act, but unlike the CCPA the MHMD Act does not provide for statutory damages, meaning plaintiffs must prove actual damages to succeed.

Sector-Specific Enforcement

In addition, a wide range of sector-specific regulators, particularly those in the healthcare, financial services, telecommunications and insurance sectors, have authority to issue and enforce privacy and security regulations, with respect to entities under their jurisdiction.

REGISTRATION

There is no requirement to register databases or personal information processing activities. However, four states currently impose certain registration requirements on data brokers:

California

The CCPA (as amended in 2019) requires (subject to some exceptions) that data brokers register with the California Attorney General (however, following amendments to the data broker registration law in late 2023, the data broker registration process and list is being transferred to the Agency). Under the law, a "data broker" is defined as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. The terms "sell" and "personal information" are defined as set forth in the CCPA.

Oregon

In 2023, Oregon passed a law requiring data brokers register on an annual basis with the Department of Consumer and Business Services before collecting personal data in Oregon. Companies must register if they maintain data that is “categorized or organized for sale or licensing to another person.” The law took effect on January 1, 2024.

Texas

In 2023, Texas passed a law requiring data brokers register with the Secretary of State. The law has a narrower scope than most of the other state data broker registration laws in that it only applies to businesses that (1) in a 12-month period, derive more than 50% of their revenue from the processing or transfer of personal data that the business did not collect directly from individuals, or (2) derive revenue from the processing or transfer of personal data of more than 50,000 individuals whose data the business did not directly collect. The law took effect on September 1, 2023, with first registrations due March 1, 2024.

Vermont

In 2018, Vermont passed a law requiring data brokers to register with the Secretary of State and adhere to minimum data security standards. Under the law a “data broker” is defined as a company that collects computerized, personal information of Vermont residents with whom the company has no direct relationship, and either sell or licenses that information.

In addition, several state laws require entities that engage in certain types of telemarketing activities to register with the state attorney general or other consumer protection agency.

DATA PROTECTION OFFICERS

With the exception of entities regulated by HIPAA, there is no general requirement to appoint a formal data security officer or data privacy officer.

Massachusetts and some other state laws and federal regulations, including the recently updated FTC Safeguards Rule (applicable to non-banking financial institutions), require organizations to appoint one or more employees to maintain their information security program.

COLLECTION & PROCESSING

US privacy laws and self-regulatory principles vary widely, but generally require that a notice be provided or made available pre-collection *(eg,* in a privacy policy) that discloses a company's collection, use and disclosure practices, the related choices individuals have regarding their personal information, and the company's contact information.

Opt-in consent is required under certain circumstance to collect, use and disclose certain sensitive data, such as health information, credit reports, financial information, children’s personal information, biometric data, video viewing choices, geolocation data and telecommunication usage information.

All states with comprehensive privacy laws, other than California, Florida, Iowa, and Utah require a business obtain consent from consumers to collect their sensitive data. California requires businesses to provide individuals a right to limit use of their sensitive data, and Iowa and Utah require individuals be provided a notice and right to opt-out of the collection of sensitive data.

The (federal) Children’s Online Privacy Protection Act (COPPA) requires verifiable parental consent prior to the collection of any personal information from children under 13. In addition, the CCPA requires that a business obtain explicit consent prior to the sale of any personal information about a consumer that the business has "actual knowledge" is less than 16 years old, and where the consumer is less than 13 years old, express parental authorization is required. (As discussed further below, the definition of "sale" under the CCPA is very broad and may include online advertising and retargeting activities, for example.). Amendments to the CCPA expanded this concept to include “sharing” of a minor’s personal information (meaning the disclosing of personal information for purposes of cross-contextual behavioral advertising).

Further, companies generally need to obtain opt-in consent prior to using, disclosing or otherwise processing personal information in a manner that is materially different than what was disclosed in the privacy policy applicable when the personal information was initially collected. The FTC deems such changes ‘retroactive material changes’ and considers it

unfair and deceptive to implement a retroactive material change without obtaining prior, affirmative consent. Under the CCPA, which applies to individual and household data about California residents, businesses must, among other things:

- At or before collection, provide a notice to consumers disclosing the categories of personal information to be collected. the purposes for collecting such information, whether such information will be sold or shared, and how long such information will be retained or the criteria to determine such period.
- Post a privacy policy that discloses
    - the categories of personal information collected, categories of personal information disclosed for a business purpose, and categories of personal information "sold" and "shared" by the business in the prior 12 months
    - the purposes for which the business collects, uses, sells, and shares personal information
    - the categories of sources from which the business collects personal information
    - the categories of third parties to whom the business discloses personal information and
    - the rights consumers have regarding their personal information and how to exercise those rights
- Include a “do-not-sell-or-share my information” link on the business's website and page where consumers can opt-out of the sale and sharing of their personal information (if applicable)
- Generally, provide at least two methods for consumers to submit CCPA requests to the business, including an online method (e.g., submission of an online form) and a toll-free number

Other California privacy laws (*eg*, the California “Shine the Light Law” and the California Online Privacy Protection Act) currently in force impose additional notice obligations, including:

- Where any personal information is disclosed to a third party for their own marketing use, a specific notice about such disclosure (*eg*, in a company’s privacy policy) must be provided and accessible through a special link on their homepage. Further, the law gives California residents to request a list of the personal information and third parties to whom such information was disclosed for marketing purposes in the prior 12 months
- Whether the company honors any do-not-track mechanisms

Under the comprehensive US state privacy laws , individuals have various qualified rights to request access to, correction, and deletion of their personal information and to “opt out” of sales, sharing, and the use of their personal information for targeted advertising purposes. Further, these laws require businesses to conduct data protection or risk assessments before engaging in certain higher-risk processing activities, such as processing that relates to:

- Certain unfair or intrusive profiling or targeted advertising purposes
- Selling of personal data
- Processing sensitive data

All states other than California and Utah require businesses to establish an internal process whereby consumers may appeal a controller’s refusal to take action on a privacy request and, where the appeal is denied, a method by which the consumer can submit a complaint to the state’s Attorney General.

Other states impose a wide range of specific requirements, particularly in the student and employee privacy areas. For example, a significant number of states have enacted employee social media privacy laws, and, in 2014 and 2015, a disparate array of education privacy laws. In addition, there are several sector-specific privacy laws that impose notice obligations, significantly limit permitted disclosures of personal information, and grant individuals the right to access or review records about the individual that are held by the regulated entity.

The US also regulates marketing communications extensively, including telemarketing, text message marketing, fax marketing and email marketing (which is discussed below).

TRANSFER

There are generally no geographic transfer restrictions that apply in the US, except regarding the storing of some governmental records and information. However, the HIPAA Privacy Rule requires that covered entities not disclose protected health information outside the US without appropriate safeguards.

SECURITY

Most US businesses are required to take reasonable technical, physical and organizational measures to protect the security of sensitive personal information (*eg*, health or financial information, telecommunications usage information, biometric data, or information that would require security breach notification). A few states have enacted laws imposing more specific security requirements for such data.

For example, Massachusetts has enacted regulations that apply to any company that collects or maintains sensitive personal information (*eg*, name in combination with Social Security number, driver's license, passport number, or credit card or financial account number) on Massachusetts residents. Among other things, the Massachusetts regulations require regulated entities to have a comprehensive, written information security program and set forth the minimum components of such program, including binding all service providers who touch this sensitive personal information to protect it in accordance with the regulations. Massachusetts law includes encryption requirements on the transmission of sensitive personal information across wireless networks or beyond the logical or physical controls of an organization, as well as on sensitive personal data stored on laptops and portable storage devices.

Some states impose further security requirements on payment card data and other sensitive personal information. In 2019, New York passed a new law (the New York “SHIELD Act”) setting forth minimum security obligations for safeguarding private information. The SHIELD Act does not mandate specific safeguards but rather provides that a business will "be deemed to be in compliance" with the law if it implements a security program that includes elements set forth in the SHIELD Act.

The CCPA and Washington’s MHMD Act provide a private right of action to individuals for certain breaches of unencrypted personal information or consumer health data, respectively, which increases class action risks posed by data breaches.

There are also several other sectoral data security laws and regulations that impose specific security requirements on regulated entities – such as in the financial, insurance and health sectors. Federal financial regulators impose extensive security requirements on the financial services sector, including requirements for security audits of all service providers who receive data from financial institutions. For example, the New York Department of Financial Services (NYDFS) regulations impose extensive cybersecurity and data security requirements on licensees of the NYDFS, which includes financial services and insurance companies. The federal Gramm-Leach-Bliley Act and implementing rules and regulations require financial institutions to implement reasonable security measures.

HIPAA regulated entities are subject to much more extensive data security requirements. HIPAA security regulations apply to so-called ‘covered entities’ such as doctors, hospitals, insurers, pharmacies and other healthcare providers, as well as their ‘business associates’ which include service providers who have access to, process, store or maintain any protected health information on behalf of a covered entity. ‘Protected health information’ under HIPAA generally includes any personally identifiable information collected by or on behalf of the covered entity during the course of providing its services to individuals.

Internet of Things

California enacted the first US Internet of Things (IoT) legislation, effective January 1, 2020. Under SB 327, manufacturers of most IoT and Bluetooth connected devices will be required to implement reasonable security features ‘appropriate to the nature and the function of the device and the information the device may collect, contain or transmit’ and ‘ designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.’ To the extent a device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature if (i) the preprogrammed is unique to each device manufactured, or (ii) the device forces the user to set a unique password upon first use.

BREACH NOTIFICATION

All 50 US states, Washington, DC, and most US territories (including, Puerto Rico, Guam and the Virgin Islands) have passed breach notification laws that require notifying state residents of a security breach involving more sensitive categories of

information, such as Social Security numbers and other government identifiers, credit card and financial account numbers, health or medical information, insurance ID, tax ID, birthdate, as well as online account credentials, digital signatures and/or biometrics.

Under many state laws, where more than 500 individuals are impacted, notice must also be provided to credit bureaus. Nearly half of states also require notice to state Attorneys General and / or other state officials of certain data breaches. Further, certain states require impacted individuals to be provided with credit monitoring services for specified lengths of time if the breach involved Social Security numbers. Finally, some state data breach laws impose certain (varying) notice content and timing requirements with respect to notice to individuals and to state Attorneys General and/or other state officials.

Federal laws require notification in the case of breaches of healthcare information, breaches of information from financial institutions, breaches of telecom usage information held by telecommunication providers, and breaches of government agency information.

ENFORCEMENT

Various entities enforce US national and state privacy laws. Violations of privacy laws and rules are generally enforced by the FTC, state Attorneys General, or the regulator for the industry sector in question. Civil penalties can be significant, particularly for uncooperative or repeat offenders.

In addition, individuals may bring private rights of action (and class actions) for certain privacy or security violations.

Some privacy laws (for example, credit reporting, marketing and electronic communications, video viewing history, call recording and cable communications privacy laws) may be enforced through private rights of action, which give rise to class action lawsuits for significant statutory damages and attorney’s fees, and individuals may bring actions for actual damages from data breaches.

The CCPA provides individuals with a private right of action and statutory damages, in the event of certain breaches of unencrypted personal information, where a business has failed to implement reasonable data security procedures (this applies to most categories of personal information under California’s breach notification law) – this raises significant class action risks. Currently, no other comprehensive state privacy laws contain a private right of action.

In June 2018, Ohio became the first US state to pass cybersecurity safe harbor legislation. Under SB 220, a company that has suffered a data breach of personal information has an affirmative defense if it has ‘created, maintained, and complied with a written cybersecurity program that contains administrative, technical, and physical safeguards to protect personal information that reasonably conforms to an industry recognized cybersecurity framework’ (*e.g.*, PCI-DSS standards, NIST Framework, NIST special publications 800-171, 800-53, and 800-53a, FedRAMP security assessment framework, HIPAA, GLBA).

ELECTRONIC MARKETING

The US regulates marketing communications extensively, including email and text message marketing, as well as telemarketing and fax marketing.

Email

The CAN-SPAM Act is a federal law that applies labeling and opt-out requirements to all commercial email messages. CAN-SPAM generally allows a company to send commercial emails to any recipient, provided the recipient has not opted out of receiving such emails from the sender, the email identifies the sender and the sender’s contact information, and the email contains instructions on how the recipient can easily and without cost opt out of future commercial emails from the sender. The FTC and state Attorneys General, as well as ISPs and corporate email systems can sue violators. Knowingly falsifying the origin or routing of a commercial email message is a federal crime.

Text Messages

Federal and state regulations apply to the sending of marketing text messages to individuals. Express consent is required to send text messages to individuals, and, for marketing text messages, express written consent is required (electronic written consent is

sufficient, but verbal consent is not). The applicable regulations also specify the form of consent. This is a significant class action risk area, and any text messaging (marketing or informational) program needs to be carefully reviewed for strict compliance with legal requirements.

Calls to Wireless Phone Numbers

Similar to text messages, federal and state regulations apply to marketing calls to wireless phone numbers. Prior express consent is required to place phone calls to wireless numbers using any autodialing equipment, and, for marketing calls, express written consent is required (electronic written consent is sufficient, but verbal consent is not). The applicable regulations also specify the form of consent. This is a significant class action risk area, and any campaign or program that involves calls (marketing or informational) to phone numbers that may be wireless phone numbers needs to be carefully reviewed for strict compliance with legal requirements. The definition of autodialing equipment is generally considered to, broadly, include any telephone system that is capable of (whether or not used or configured storing or producing telephone numbers to be called, using a random or sequential number generator.

Telemarketing

Beyond the rules applicable to text messaging and calling to wireless phone numbers, there are federal and state telemarketing laws as well. Federal telemarketing laws apply to most telemarketing calls and programs, and state telemarketing law will apply to telemarketing calls placed to or from within that particular state. As a result, most telemarketing calls are governed by federal law, as well as the law of one or more states. Telemarketing rules vary by state, and address many different aspects of telemarketing, such as calling time restrictions, do-not-call registries, opt-out requests, mandatory disclosures, requirements for completing a sale, executing a contract or collecting payment during the call, further restrictions on the use of auto-dialers and pre-recorded messages, and record-keeping requirements. Many states also require telemarketers to register or obtain a license to place telemarketing calls.

Fax Marketing

Federal law and regulations generally prohibit the sending of unsolicited advertising by fax without prior, express consent. Violations of the law are subject to civil actions and have been the subject of numerous class action lawsuits. The law exempts faxes to recipients that have an established business relationship with the company on whose behalf the fax is sent, as long as the recipient has not opted out of receiving fax advertisements and has provided their fax number ‘voluntarily,’ a concept which the law specifically defines.

The law also requires that each fax advertisement contain specific information, including:

- A ‘clear and conspicuous’ opt-out method on the first page of the fax
- A statement that the recipient may make a request to the sender not to send any future faxes and that failure to comply with the request within 30 days is unlawful, and
- A telephone number, fax number, and cost-free mechanism to opt-out of faxes, which permit consumers to make opt-out requests 24 hours a day, seven days a week
- Violations are subject to a private right of action and statutory damages, and thus pose a risk of class action lawsuits

ONLINE PRIVACY

There is no specific federal law that *per se* regulates the use of cookies, web beacons and other similar tracking mechanisms. However, the state online privacy laws require notice of online tracking and of how to opt out of it.

Under California law, any company that tracks any personally identifiable information about consumers over time and across multiple websites must disclose in its privacy policy whether the company honors any ‘Do-Not-Track’ method or provides users a way to opt out of such tracking. The same law also requires website operators to disclose in their privacy policy whether any third parties may collect any personally identifiable information about consumers on their website and across other third party websites, and prohibits the advertising of certain products, services and materials (including alcohol, tobacco, firearms,

certain dietary supplements, ultraviolet tanning, tattoos, obscene matters, etc.). Further, under most of the comprehensive state laws, information collected via cookies, online, mobile and targeted ads, and other online tracking are subject to the requirements of the law.

Further, given the broad definition of personal information under the comprehensive state privacy laws, information collected via cookies and similar technologies is generally subject to the requirements of the law (e.g., notice and consumer rights). For example, under the CCPA a 'sale' includes selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating a consumer’s personal information by one business to another business or a third party for monetary or other valuable consideration. ‘Sharing’ under the CCPA is defined as sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged. These broad definitions sweep in certain online advertising activities -- for example, where a business permits the collection and use of information through certain third party cookies and tags on their website, in order to better target the business' ad campaigns on third party websites or in exchange for compensation from a third party ad network.

Universal Opt-Out Signals / Global Privacy Control (GPC)

Amendments to the CCPA, and recent enforcement actions by the California Attorney General, have highlighted the requirement that businesses that process personal information for targeted advertising purposes allow consumers to opt-out of sales and sharing, using an opt-out preferences signal sent by the consumer’s browser or a browser plugin, aso referred to as Global Privacy Control (GPC). Colorado’s comprehensive privacy law introduces the same requirement, with an effective date of July 1, 2024.

Minors

The Children’s Online Privacy Protection Act and regulations (COPPA) applies to information collected automatically (*eg*, via cookies) from child-directed websites and online services and other websites, online services and third party ad networks or plug-ins that knowingly collect personal information online from children under 13. COPPA also regulates behavioral advertising to children under 13 as well as the collection of geolocation information, requiring prior verifiable parental consent to engage in such advertising or collection.

California law requires that operators of websites or online services that are directed to minors or that knowingly collect personally identifiable information from minors permit minors that are registered users of their sites to remove any content the minor has posted from the site or online service. The law does not give minors the right to remove information posted by third parties. Minors must be given clear notice on how to exercise their right to removal. Certain state privacy laws (such as the CCPA, CPA or VCDPA) also require that a business obtain explicit consent prior to selling any personal information about an individual the business has actual knowledge is under 16 years old.

Location Data

Generally, specific notice and consent in needed to collect precise *(e.g.,* mobile device) location information. The CCPA defines precise geolocation information as “any data derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of one thousand, eight hundred and fifty (1,850) feet.” Connecticut and Utah law carry similar definitions, albeit with a radius of 1,750 feet.

KEY CONTACTS

Kate Lucente
Partner and Co-Editor, Data Protection Laws of the World
T +1 813 222 5927
kate.lucente@dlapiper.com

Andrew Serwin
Partner, Global Co-Chair Data Protection, Privacy and Security Group
T +1 858 677 1418
andrew.serwin@dlapiper.com

Jennifer Kashatus
Partner
T +1 202 799 4448
jennifer.kashatus@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

URUGUAY

Last modified 28 January 2024

LAW

Data Protection Act Law No. 18.331 (11 August 2008); Decree No. 414/009 (31 August 2009), Arts 47 to 40, Act Law No. 19.670 (15 October 2018), Decree No. 64/2020 (17 February 2020) and Arts 62 and 63, Act No. 20.075 (20 October 2022). .

DEFINITIONS

Definition of personal data

Any kind of information related to an individual or legal entity identified or identifiable.

Definition of sensitive personal data

Any kind of personal data evidencing: racial or ethnic origin, political preferences, religious or moral beliefs, trade union membership and any kind of information concerning health or sexual life.

NATIONAL DATA PROTECTION AUTHORITY

(“**URCDP**”), *Unidad Reguladora de Control y Actos Personales* (“**Data Protection Authority**”).

REGISTRATION

The Uruguayan legal system requires the registration of all databases containing personal data of individuals or legal entities (Articles 24, 28, and 29 of the Act and Articles 15 to 20 of the Decree 414/009).

The Law applies when the processing of personal data is performed by controllers located in Uruguay.

The Act has extraterritorial effects in the following cases:

- if the activities are related to the offer of goods or services to individuals residing in Uruguay, or intended to monitor their behaviour;
- if private international laws or contractual agreements so establish it; and
- if the processing is made by using means located in Uruguay, with the exceptions of the cases in which those means are used for the sole purpose of transit, and there is a person responsible for the processing with residency in Uruguay, appointed by the controller before the URCDP.

The register must be updated every three months (Article 20 of the Decree 414/009).

DATA PROTECTION OFFICERS

The appointment of a Data Protection Officers (DPO) is mandatory in the following cases: (i) public state or non-state entities, (ii) private or partially state-owned entities, (iii) private entities which process sensitive data as a core activity, and (iv) private entities which process large scales of data.

Decree 64/2020 clarifies that large scales of data means the data processing of more than 35,000 subjects.

The DPO must meet the conditions required for the correct performance of his/her duties. He/she must act autonomously in technical matters.

The appointment of a DPO must be submitted before the URCDP for its approval. If the legal and technical requirements are not met, the Regulator is entitled to deny or revoke (as the case may be) the filing/authorisation to the appointed DPO.

COLLECTION & PROCESSING

In order to collect the information which is contained in the database, the data processor should obtain prior documented consent from the individual or entity whose information is being processed. Documented consent is not required in the following cases:

- personal data obtained from public sources;
- personal data obtained by public bodies to comply with legal obligations;
- personal data limited to domicile, telephone number, ID number, nationality, tax number, corporation name;
- personal data obtained in base of a contractual or professional relationship, which is necessary to perform the contract or the development of the professional services to be rendered; and
- personal data obtained by individuals or corporations for their personal and exclusive use.

The personal data processed cannot be used for purposes different from those that have justified the acquisition of the information. It is understood that legitimate reasons (i.e. reasons which are not against the law) must pre exist and underlay the processing of the personal information. The Data Protection Act further establishes that once the reasons to process the personal information have disappeared, the personal information must be deleted.

Data subjects have the right to be informed by the data processor about how their information is and has been used, and may exercise this right at all times.

TRANSFER

Personal data can only be transferred to a third party:

- for the compliance of purposes directly related to the legitimate interest of the transferring party and the transferee; and
- with the data subject's prior consent. Such consent may be revoked. Additionally, the data subject must be informed of the purpose of the transfer, the identity of the transferee, and the purposes for which the personal data will be used

The data subject's prior consent is not necessary if the individual’s data to be transferred is limited to: name, surname, identity card number, nationality, address, and date of birth.

The purpose and proper identification of the transferee must be included in the consent communication that would be addressed to the data subject. Evidence of the data subject’s consent must be kept in the files of the data processor.

If the data subject’s consent is not obtained within ten business days (counted from the receipt of the communication from the data processor asking for the consent), it will be construed that the data subject did not consent to the transfer of the data.

Upon the transfer, the data processor will remain jointly and severable liable for the compliance of the transferee obligations under the Data Protection Act.

The Data Protection Act forbids the transfer of personal data to countries or international entities which do not provide adequate levels of data protection (according to URCDP). However, the Data Protection Act allows international transfer to

unsafe countries or entities, when the data subject consents to the transfer (such consent must be given in writing), or when the guarantees of adequate protection levels arise from “contractual clauses”, and “self regulation systems”. The international data transfer agreement must establish the same levels of protection which are effective under the laws of Uruguay.

In the case of a cross‑border transfer within a group of companies, Uruguayan laws establish that the international transfer will be lawful without any authorisation whenever the branch has the same conduct code duly registered before the local URCDP.

The international transfer of personal data between headquarters and their respective branches or subsidiaries is authorised when the headquarters and their branches have a conduct code duly filed before URCDP.

SECURITY

The data processor must implement appropriate technical and organisational measures to guarantee the security and confidentiality of the personal data. These measures should be aimed at avoiding the loss, falsification, non‑authorised treatment or inquiry, as well as at detecting information that may have been leaked, performed by human intervention or not.

It is forbidden to register personal data in databases which do not meet technical safety conditions.

BREACH NOTIFICATION

Data breaches and data incidents must be reported to the URCDP and to the Data Subject.

Once the DPO or the Data Controller confirms the occurrence of a security breach, it must be notified to the URCDP within 72 hours.

Notification to data subjects must be done once the DPO or the Data Controller confirms the occurrence of a security breach. The Uruguayan Data Privacy Act requires the notification to be effected “as soon as practicable”, but fails to spell out a precise time frame for such notice.

Legal requirement of the data breach/incident

- Notification to the Regulator must contain relevant information, including the:
  - certain or estimated date of the occurrence of the breach;
  - main characteristics of the breach;
  - details of the data affected; and
  - the possible impacts.
- The regulation does not state any formalities to the communication to the Data subject. However, it states that such notification must be clear and simple.

After the first notification to the Regulator within the first 72 hours after the Data Breach/incident, a second communication must be done by the DPO or the Data Controller to the Regulator. The second report must indicate all the details of what happened and the measures that were adopted and carried out so that such violation/incident has been mitigated and does not occur again. The Act does not state a time frame for execution of the second report.

ENFORCEMENT

The URCDP is responsible for the enforcement of the Data Protection Act. In the context of its powers, the URCDP is entitled to:

- request the data processor the exhibition of books, documents and files, electronic or not;
- summon the data processor before the URCDP in order to provide information;
- intervene in the documents and files inspected;
- adopt security or protection measures in order to preserve the documentation, including copying the files;
- seize or impound the documents and files for six days;

- carry out inspections on data processor’s offices;
- summon third parties to appear before the URCDP.

The URCDP has the authority to impose penalties against the data processor in the following order: warning, admonition, fines up to USD 60,000, suspension of the data base during five days, and closure of the database.

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as these activities likely involve the processing and use of personal data (e.g. an email address is likely to be "personal data" for the purposes of the Act). The Act does not prohibit the use of personal data for the purposes of electronic marketing but grants personal data owners with the right to demand the elimination or blocking of their data from the data base.

Personal data can be used and processed for marketing purposes when it has been taken from public documents, when it has been provided by the personal data owner or when prior consent has been gathered.

ONLINE PRIVACY

There are no express provisions for online privacy, but the general data privacy principles fully apply. In this regard, key principles such as prior informed consent, the purposes of collection and use, and the right to information are particularly relevant. These principles state that in order to use cookies, the data subject's prior consent must be obtained and the data subject must be informed about the purposes of collection and use; personal data collected through cookies may only be processed as necessary to fulfill the purposes for which it was collected and must be deleted when the purpose ceases.

KEY CONTACTS

Bergstein Abogados
www.bergsteinlaw.com/

Jonás Bergstein
Partner
Bergstein Abogados
jbergstein@bergsteinlaw.com

Ignacio Torres Negreira
Senior Associate
Bergstein Abogados
itorresnegreira@bergsteinlaw.com

Guzman Ramírez
Senior Associate
Bergstein Abogados
T (598) 2 901 2448
gramirez@bergsteinlaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

UZBEKISTAN

Last modified 22 January 2024

LAW

Until recently, Uzbekistan did not have a stand-alone personal data protection law. The situation changed with the adoption on 2 July 2019 of the Law of the Republic of Uzbekistan No. ZRU-547 “On Personal Data” (“**Law on Personal Data**”), which entered into force on 1 October 2019.

With the entry into force of the Law on Personal Data, a unified set of main rules and requirements in the area of data protection and processing that is aimed at substantial regulation of these issues was introduced in Uzbekistan.

The scope of application of this Law is rather broad, as it applies to *relations arising from processing and protection of personal data, regardless of the applied means of processing, including information technologies*.

Apart from the Law on Personal Data, there are certain legal acts that establish fundamental principles of data protection processing and / or set liability for violation of data protection rules. They include:

- Constitution of the Republic of Uzbekistan (in the new edition), effective from 1 May 2023;
- Civil Code of the Republic of Uzbekistan, effective from1 March 1997;
- Labour Code of the Republic of Uzbekistan (in the new edition), effective from 30 April 2023;
- Code of the Republic of Uzbekistan on Administrative Liability, effective from 1 April 1995 (‘Code on Administrative Liability’);
- Criminal Code of the Republic of Uzbekistan, effective from 1 April 1995 (‘Criminal Code’);
- Law No. 439-II 'On Principles and Guarantees of Freedom of Information' dated December 12, 2002; and
- Law No. 560-II 'On Informatization' dated December 11, 2003.

Lastly, there are also sector-specific laws applicable depending on the type of industry. Data protection regulation exists mainly in financial, telecommunication, health and insurance sectors and consists of the following legal acts:

- Law No. 530-II 'On Bank Secrecy' dated August 30, 2003, under which a bank is prohibited to disclose bank secrecy, and should guarantee its protection;
- Law No. 822-I 'On Telecommunications' dated August 20, 1999, under which all operators and service providers are obliged to ensure the secrecy of communications;
- Law No. 265-I 'On Protection of Citizens’ Health' dated August 29, 1996, under which the medical secrecy is protected; and
- Law No. ZRU-730 'On Insurance Activities' (in the new edition) dated November 23, 2021, under which insurance companies should guarantee the confidentiality of information which became available in course of provision of insurance services.

DEFINITIONS

Definition of personal data

The Law on Personal Data defines **Personal Data** as information recorded on electronic, paper and / or other tangible medium, relating to a specific individual or that allows to identify such individual (i.e. ‘**subject of personal data**’).

Apart from the above, the Law on Personal Data distinguishes separate types of personal data in respect of which the Law imposes a special processing and protection regime. They include:

- **special personal data**, i.e. data about racial or social origin, political, religious or ideological beliefs, membership in political parties and trade unions, as well as data regarding physical or mental health, information about private life and criminal records;
- **biometric personal data**, i.e. personal data characterizing anatomical and physiological characteristics of the subject of personal data; and
- **genetic personal data**, i.e. personal data related to the inherited or acquired characteristics of the subject of personal data, which is the result of the analysis of the biological sample of the subject or the analysis of another element that allows to obtain equivalent information.

Definition of sensitive personal data

The Law on Personal Data does not provide for an express definition of sensitive personal data. Yet, it distinguishes the category of *special personal data*. Under the foregoing Law, special personal data includes:

- data about racial or social origin;
- data about political, religious or ideological beliefs;
- data about membership in political parties and trade unions;
- data about physical and mental health; and
- data about private life and criminal records.

NATIONAL DATA PROTECTION AUTHORITY

The Law on Personal Data designates the Cabinet of Ministers of the Republic of Uzbekistan (the '**Cabinet of Ministers**') and State Personalization Centre under the Cabinet of Ministers (the ‘**State Personalization Centre**’) as the main regulatory authorities in respect of the protection of personal data. That said, following the recent administrative reform, the State Personalization Centre was reorganised into the Personalization Agency under the Ministry of Justice of the Republic of Uzbekistan (the '**Personalization Agency**’).

Additionally, following the latest amendments to Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 707 “On Measures for Further Improvement of Information Security in Internet” dated September 5, 2018 (“ **Resolution No. 707**”) adopted in pursuance of the recently introduced localization requirement, the State Inspection of the Republic of Uzbekistan on Informatization and Telecommunication was designated as a state authority empowered, *inter alia*, to:

- implement the state control over the activity of personal database owners and operators by monitoring their activities;
- issue notifications, instructions, as well as orders that are to be fulfilled by public authorities, individuals and / or legal entities, in order to ensure compliance with the data protection laws;
- maintain the Register of Infringers of the Rights of Personal Data Subjects.

REGISTRATION

The Law on Personal Data requires a personal data database to be registered with the State Registry of Personal Databases maintained by the Personalization Agency. The registration should represent a simple notification with the Personalization Agency.

The registration is performed by an owner / operator of personal database by way of notification, i.e. by approaching the Personalization Agency in person or via its website (Government registry for personal databases).

The registration procedure for personal database is mainly set forth by the Regulation on the State Register of Personal Databases, approved by the Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 71 dated February 8, 2020 (‘**Regulation No. 71**’).

Under Regulation No. 71, to register a personal database, an owner / operator of personal data is required to fill and submit the application as per the prescribed form to the Personalization Agency. In its turn, the Personalization Agency shall review the submitted application within 15 days from the date of its receipt. Based on the results of such review, the Personalization Agency either agrees or refuses to register the database. In case of a positive decision, the Personalization Agency issues a certificate on registration of a personal database to an owner / operator of personal data.

The registration is not required for databases containing personal data:

- relating to participants / members of a public association or religious organization and processed accordingly by a public association or religious organization, provided that personal data will not be distributed or disclosed to third parties;
- made by the subject of personal data publicly available;
- that constitutes only last name, first name and patronymic of the subject of personal data;
- necessary for the purposes of a single access authorization of the subject of personal data to the territory where the owner and / or operator is located, or for other similar purposes;
- included in personal data information systems with the status of state automatized information systems;
- processed without the use of automation technology;
- processed in accordance with labour laws.

DATA PROTECTION OFFICERS

According to the Law on Personal Data, government bodies, legal entities and individuals processing personal data (i.e. **operators of personal data**) or having the right to use and dispose personal data (i.e. **owners of personal data**) must designate a structural unit or a responsible person that has to organize work with respect to personal data protection in the course of its processing.

COLLECTION & PROCESSING

Under the Law on Personal Data, processing of personal data includes actions with respect to:

- Collection;
- Systematization;
- Storage;
- Modification;
- Addition;
- Use;
- Provision;
- Dissemination;
- Transfer;
- Depersonalization; and
- Destruction.

Further, the Law on Personal Data stipulates 7 grounds / conditions for processing of personal data, as follows:

- upon the subject’s consent to processing of his / her personal data;
- when processing of the subject’s personal data is necessary to fulfil the agreement to which the subject is a party to, or to take measures at the request of the subject before concluding such agreement;
- when processing of the subject’s personal data is required for fulfilment of obligations of the owner and / or operator as defined by law;
- when processing of the subject’s personal data is necessary for protection of legitimate interests of the subject or other person;

- when processing of the subject’s personal data is required to exercise the rights and legitimate interests of the owner and / or operator or a third party, or in order to achieve socially significant goals, provided that the subject’s rights are not violated;
- when processing of the subject’s personal data is necessary for statistical or other research purposes, under the mandatory condition of depersonalization of personal data;
- if the subject’s personal data is taken from public sources.

Processing of personal data should pursue a certain purpose. This purpose should be fixed in legal acts, regulations, charter or other documents regulating the activities of the owner / operator of personal data. That said, the owner / operator should specify in its foundation documents or other internal documents (e.g. data privacy policy etc.) the purpose of data processing. Whenever the purpose of these operations changes, a new consent from the subject to conduct operations over the personal data related to them in line with such new purpose must be obtained.

In order to achieve the intended purpose of personal data processing, the owner / operator has the right to independently determine the procedure and principles of collection and systematization of personal data. Therefore, the volume and the nature of personal data to be processed should correspond to the purpose and applied methods of processing.

According to the Law on Personal data, the owner / operator may assign the processing of personal data to third parties in the following cases:

- upon the subject’s consent obtained in a written form or in the form of an electronic document;
- if such assignment is made based on an agreement between the owner and the subject of personal data or for the fulfilment of the conditions of an existing agreement;
- other cases stipulated by law.

In processing the personal data, the owner / operator must comply with notification requirements set by the Law on Personal Data. Under the foregoing Law, the owner / operator must notify the subject:

- on inclusion of the subject’s personal data into the personal database along with informing the subject on purpose of personal data processing and the subject’s respective rights. The period of notification is not defined by the Law on Personal Data;
- on transfer of the subject’s data to third parties. Such notification must be provided within a 3-day period;
- upon the subject’s application. Under the Law on Personal Data, the subject has the right to request the owner / operator to provide him / her with information about processing of his / her data.

Upon achievement of the processing purpose, as well as in other cases stipulated by the Law on Personal Data (e.g. withdrawal of the subject’s consent, decision of the court etc.) personal data is subject to destruction by the owner / operator.

Along with the above, on 15 January 2021 data localization requirement was introduced to the Law on Personal Data that came into force on 16 April 2021. Under this requirement the personal data of Uzbek citizens processed with the use of information technologies, including via the Internet, must be collected, systematized and stored on technical means physically located on the territory of Uzbekistan and in databases duly registered in the State Register of Personal Databases.

TRANSFER

The Law on Personal Data defines the cross-border transfer of personal data as the transfer of personal data by the owner / operator outside the territory of the Republic of Uzbekistan. Cross-border transfer of personal data is allowed only to the territory of foreign states providing adequate protection of the rights of personal data subjects. At present, it is unclear which states will qualify as providing “adequate” protection, as no list of such countries has been adopted yet by the regulatory authorities.

Nevertheless, cross-border transfer of personal data is still possible even if the foreign state does not provide the adequate protection. Such transfer is possible in 3 exceptional cases:

- the subject explicitly agrees to such transfer;

- there is a need to protect the constitutional order of Uzbekistan, the public order, rights and freedoms of citizens, health and morality of the population;
- if such transfer is stipulated by the international treaty of Uzbekistan.

The Law on Personal Data also determines that cross-border transfer of personal data may be prohibited or restricted in order to protect the constitutional order of the Republic of Uzbekistan, morality, health, rights and legitimate interests of citizens, and to secure defense of the country and national security.

SECURITY

The Law on Personal Data states that personal data is subject to the protection guaranteed by the State. It also imposes obligations on the owner / operator of personal data and the third party acquiring personal data to take necessary legal, organizational and technical measures ensuring:

- non-interference into the subject's private life;
- integrity and safety of personal data;
- confidentiality of personal data;
- prevention of illegal processing of personal data.

Obligations of the owner / operator of personal data on protection of confidentiality of personal data arise from the moment such data is collected until their destruction or depersonalization.

The owner / operator of personal data shall take organizational and technical measures to protect personal data based on the potential threats to their security.

Threats to the security of personal data are defined as a combination of conditions and factors that may lead to their alteration, addition, use, provision, transfer, dissemination, depersonalization, destruction, and copying as a result of unauthorized, including accidental access to the personal database.

Please note that the recently adopted Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 570 ‘On Approval of Certain Normative Legal Documents in the Field of Processing of Personal Data’ dated 5 October 2022 approved the following regulations that came into effect on 7 January 2023:

- the Regulation on determining the levels of protection of personal data during their processing;
- the Regulation on the requirements for material carriers of biometric and genetic data and storing technologies of such data outside personal databases.

BREACH NOTIFICATION

There is no requirement on breach notification under the Law on Personal Data. However, in case of violation of data processing rules (e.g. unauthorized data processing), the owner / operator of personal data must suspend processing of personal data or destroy them.

ENFORCEMENT

Following the adoption of the Law on Personal Data, a number of amendments aimed at enforcing data protection rules, were introduced into the Code on Administrative Liability and Criminal Code.

Currently, under the Code of Administrative Liability illegal collection, systematization, storage, modification, addition, use, provision, dissemination, transfer, depersonalization and destruction of personal data, as well as non-compliance with the localization requirement leads to the imposition of an administrative fine on citizens in the amount of 7 base calculation values (“**BCV**”) (approx. USD 193) and on officials – in the amount of 50 BCV (approx. USD 1,382).

Repeated violation of data protection rules can lead to criminal liability. Under the Criminal Code illegal processing of personal data leads to the fine in the amount from 100 BCV to 150 BCV (approx. from USD 2,764 to USD 4,146), or deprivation of a certain right for up to 3 years, or correctional labour for up to 2 years.

Furthermore, under Resolution No. 707, non-compliance with localization requirement leads to inclusion of an owner / operator of personal data into the Register of Infringers of the Rights of Personal Data Subjects and blocking access to the information resources (web-sites) of an owner / operator of personal data in Uzbekistan.

Apart from the above, the Personalization Agency can issue binding orders to legal entities and individuals on elimination of violations of data protection requirements.

ELECTRONIC MARKETING

The Law on Personal Data does not specifically regulate the use of personal data in electronic marketing. However, considering that the Law on Personal Data applies to any processing of personal data this Law will also cover processing of personal data in electronic marketing.

In addition to the above, the Law of the Republic of Uzbekistan No. ZRU-792 ‘On E-Commerce’ dated 29 September 2022, coming into effect on 31 December 2022, stipulates that the terms of use of personal data in e-commerce trading may be contractually agreed by e-commerce participants.

Lastly, the Law of the Republic of Uzbekistan No. ZRU-776 “On Advertisement” (new edition) adopted 7 July 2022 and entered into force on 9 September 2022, introduced new rules for dissemination of advertisements via telecommunication networks. A prior consent of a person is now required for distribution of advertisements through telecommunication networks. Given that telecommunication networks are broadly defined by law, it is most likely that such networks also include Internet and, therefore, this rule shall also apply to distribution of advertisements via Internet.

ONLINE PRIVACY

Current data protection laws do not provide for regulation of online privacy. However, if personal data is involved and privacy issues are concerned, there are no obstacles for their application with respect to online privacy.

KEY CONTACTS

Centil Law Firm
centil.law/#

Dilshad Khabibullaev
Partner
Centil Law Firm
T +998711204778
dilshad.k@centil.law

Valeriya Ok
Senior Associate
Centil Law Firm
T +998711204778
valeriya.ok@centil.law

Islam Gulomov
Senior Associate
Centil Law Firm
T +998711204778
islam.g@centil.law

Ibrokhim Musakhodjaev
Associate
Centil Law Firm
T +998711204778

ibrokhim.musakhodjaev@centil.law

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

VENEZUELA

Last modified 12 December 2022

LAW

There is no specific legislation about data privacy or data protection in Venezuela, however, there are isolated provisions in some existing laws that regulate certain aspects related to data protection (e.g., Law on Privacy Protection of Communications, the Special Law against Computer Crimes, the Organic Law on Prevention, Conditions, and the Working Environment, and the Civil Code, Communications from the National Superintendency of Banks).

Likewise, the Constitution of the Bolivarian Republic of Venezuela (the **"Constitution")** establishes general principles that serve as a framework for the protection of information. These principles were developed by decision No. 1318 of the Supreme Court of Justice ("TSJ" for its Spanish acronyms) of August 2011, guarding the honour, privacy, intimacy, self-image, confidentiality, and reputation of individuals. The principles are:

- Principle of free will, which implies the need of a prior, free, informed, unequivocal and revocable consent for the use, and collection of personal data.

- Principle of legality, according to which the collection of personal data entails that the limitation to information self-determination
  is a result of a legal provision.

- Principle of purpose and quality, which means that the collection of personal data must respond to predetermined purposes, motives, or causes that are not contrary to constitutional and legal provisions, also a prerequisite to obtain valid consent. Data can only be extracted and treated for the fulfilment of specific, explicit, and legitimate purposes related to the activity of those who get them. This principle entails the necessary proportionality in the collection of data, which must be adequate, relevant, and not excessive.

- Principle of temporality or conservation, under which the data should be preserved until the purposes or objectives that its collection are achieved.

- Principle of accuracy and self-determination, which means that the data must be complete, accurate and up to date, in response to the real situation of the person as the data may be subject to control by the individuals whose data is collected. The interested party must have clear and expeditious procedures to obtain from the person responsible for the use or receipt of the information: the confirmation of the use of data; the purposes of such registers and its recipients; the rectification or cancellation of inaccurate, inadequate, or excessive data, and; the knowledge of such modifications by those whose wrong information has been communicated.

- Principle of foreseeability and integrity: Although the rights relating to the collection of information should be initially aimed at protecting the rights of the individuals whose information is collected, the analysis of the impact that the collection of data has on such rights cannot be isolated and without reference to data that may be collected in other

registries.

- Principle of security and confidentiality, which implies the guarantee of confidentiality, of no alteration of data by third parties, and of access to such data by the competent authorities in accordance with the law. The data must be protected from alteration, loss, accidental destruction, unauthorised access, or fraudulent use. This protection goes as far as preventing international data transfers to States whose legislation does not guarantee a level of protection similar to the one described.

- Principle of guardianship, which means that in addition to having judicial protection to enforce the right to access the information and obtain knowledge of the use of the personal data, there should be public entities that ensure the right to the protection of personal data with powers to create or implement simplified models and based on technical standards to measure the level of efficiency of the structures and procedures in place and the level of protection of the personal data.

- Principle of liability, under which a violation of the right to the protection of personal data gives rise to liability and the imposition of civil, criminal, and administrative penalties, as the case may be.

Also, Article 28 CRBV sets the right for individuals to access their personal information stored in public or private records, to know for what use such information will be recorded, and, rectify or destroy it when incorrect or when it unlawfully affects their rights. Although there is no legal regulation in this regard, the TSJ has agreed to the possibility of maintaining this information and personal data in systems or records, stored in a way that a profile of them can be done with the purpose of using the information for personal gain or for third parties, as long as the rights set in Article 28 CRBV are respected. According to this Article, a double right is guaranteed: (i) to collect information about people and their goods, and (ii) access to such information that has been collected and is reflected in the records. However, whoever collects the information or data of the individuals or their goods, shall respect the right of the people to protect their honour, privacy, intimacy, self-image, confidentiality, and reputation, all of this provided in Article 60 CRBV.

Additionally, the decision also stipulates that the particular data that someone keeps for study purposes, or for personal use or to fulfill professional objectives, which do not form a system capable of designing a total or partial profile of individuals are not subject to these principles, since they lack a general projection. However, records that, when cross-referenced with others, make it possible to outline a profile of the private life of individuals, or of their economic situation, political tendencies, etc., could be part of the records protected by the Constitution. The mere potential of intersecting and complementing the data of a registry, with the information stored in others that complete it, makes the set of records susceptible to the rights referred to in article 28 of the Constitution.

DEFINITIONS

Definition of Personal Data

There is no legal definition of “Personal Data” in Venezuelan legislation.

Nonetheless, decision No. 855 of the TSJ, of May 8, 2012, gave us the following definition of Personal Data: *“Any information related to an identified or identifiable individual”*.

Likewise, any Personal Data must be processed fairly and responsibly for particular purposes, on the basis of the data subject's consent or as a consequence of some other legitimate basis, provided by law.

Definition of Sensitive Personal Data

There is no legal definition of “Sensitive Personal Data” in Venezuelan legislation.

However, in decision No. 1335 of the TSJ, of August 8, 2011, in a case on the sensitive and personal data in a medical record, the TSJ expressed that any such data must be handled under the strictest confidentiality and privacy controls, and its content must not be disclosed.

The decision says that sensitive and personal data is a person’s most genuine and authentic assets, and, as such, is the absolute owner and holder of all that information, only that person can grant permission for its use and treatment.

Under this decision, we can conclude that any person’s intimate data can also be considered to be Sensitive Personal Data, and, as such, must be confidential, be duly guarded and only that person can grant permission for its use and treatment.

NATIONAL DATA PROTECTION AUTHORITY

There is no National Data Protection Authority in Venezuela.

REGISTRATION

There is no legal requirement to register before any National Data Protection Authority.

DATA PROTECTION OFFICERS

There is no legal requirement to appoint a Data Protection Officer.

COLLECTION & PROCESSING

The collection and processing of Personal Data must adhere to the previously explained general principles dictated by the Constitutional Chamber of the TSJ.

TRANSFER

According to the general principles dictated by the TSJ, there is a protection against the transfer of data to States whose legislation does not guarantee a level of protection similar to the one described.

In addition, in terms of labor law, the employee's consent is required to transfer personal data to third parties. There are companies that voluntarily develop their own data protection policies or apply their headquarters policies or international standards for this matter.

SECURITY

According to the general principles dictated by the Constitutional Chamber of the TSJ, there is a guarantee of confidentiality, of no alteration of data by third parties, and of access to such data by the competent authorities in accordance with the law. The data must be protected from alteration, loss, accidental destruction, unauthorised access, or fraudulent use.

BREACH NOTIFICATION

There is no legal obligation to disclose a data breach.

Mandatory Breach Notification

It is not mandatory to disclose a data breach.

ENFORCEMENT

When it comes to labor matters and records of employees, the Organic Law on Prevention, Conditions and Working Environment ("**LOPCYMAT**" for its Spanish acronym) sets forth in Article 53 the following rules on certain data and privacy protection:

- Section 10: the right of the employees to access information contained on health screenings, as well as the confidentiality of the results with respect to third parties. (According to Article 27 of the LOPCYMAT, disclosure of health results to

certain third parties is permitted with the employee's consent. Also, per Article 119 of the LOPCYMAT, failure to comply with the obligation of section 10 may result in a fine ranging from 26 to 75 tax units ("**T.U.**") for each worker exposed.

- Section 11: the confidentiality of employees' personal health data. (According to Article 120 LOPCYMAT, failure to comply with the obligation of section 11 may result in a fine ranging from 76 to 100 T.U. for each worker exposed.
- Section 16: the privacy of employee's correspondence and communications, as well as free access to all data and information relating to the employee.
- The fines or sanctions for non-compliance according to LOPCYMAT are:
    - Article 27: disclosure of health results to certain third parties is permitted with the employee's consent.
    - In addition, per Article 119, failure to comply with the obligation of section 10 may result in a fine ranging from 26 to 75 T.U. for each worker exposed.
    - Article 120: failure to comply with the obligation of section 11 may result in a fine ranging from 76 to 100 T.U. for each worker exposed.

ELECTRONIC MARKETING

Electronic Marketing is allowed, but any collection and processing of Personal Data must adhere to the previously explained general principles dictated by the TSJ.

ONLINE PRIVACY

There is no specific legislation about online privacy in Venezuela, but we advise to adhere to the previously explained general principles dictated by the TSJ if there is going to be any processing or collection of Personal Data.

KEY CONTACTS

InterJuris Abogados S.C
interjuris.com/

Maria Cecilia Rachadell
Partner
InterJuris Abogados S.C
T +13059271390
maria.rachadell@interjuris.com

Juan José Delgado
Partner
InterJuris Abogados S.C
T +13057971121
juanjose.delgado@interjuris.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

VIETNAM

Last modified 18 January 2024

LAW

In 2023, Vietnam passed its first comprehensive data protection law, namely Decree No. 13/2023/ND-CP of the Government dated 17 April 2023 on Personal Data Protection (“**PDPD**”). However, the PDPD does not supersede data protection rights and obligations set out under other legislations in Vietnam. In particular, the right of privacy and the right of reputation, dignity and honour, and the fundamental principles of such rights, are provided for in the Constitution 2013 ("**Constitution**") and Civil Code 2015 ("**Civil Code**") as inviolable and protected by law.

Regarding personal information, the key principles on collection, storage, use, process, disclosure or transfer of personal information are specified in the following main laws and guiding documents, among others:

- Criminal Code No. 100/2015/QH13, passed by the National Assembly on 27 November 2015; as amended from time to time ("**Criminal Code**");
- Law No. 24/2018/QH14 on Cybersecurity, passed by the National Assembly on 12 June 2018 ("**Cybersecurity Law**"); Law No. 86/2015/QH13 on Network Information Security, passed by the National Assembly on 19 November 2015; as amended by Law No. 35/2018/QH14 dated 20 November 2018, on amendments to some articles concerning planning of 37 Laws ("**Network Information Security Law**");
- Law No. 19/2023/QH15 on Protection of Consumers' Rights, passed by the National Assembly on 20 June 2023 ("**CRPL**");
- Law No. 67/2006/QH11 on Information Technology, passed by the National Assembly on 29 June 2006; as amended by Law No. 21/2017/QH14 dated 14 November 2017 on planning ("**IT Law**");
- Law No. 51/2005/QH11 on E-transactions, passed by the National Assembly on 29 November 2005 ("**E-transactions Law**");
- Decree No. 13/2023/ND-CP of the Government dated 17 April 2023 on Personal Data Protection (“**PDPD** ”);
- Decree No. 53/2022/ND-CP of the Government dated 15 August 2022 elaborating a number of articles of the Law on Cybersecurity of Vietnam ("**Decree 53**");
- Decree No. 85/2016/ND-CP dated 1 July 2016, on the security of information systems by classification ("**Decree 85**"); Decree No. 72/2013/ND-CP dated 15 July 2013 of the Government, on management, provision and use of Internet services and online information; as amended by Decree No. 27/2018/ND-CP dated 1 March 2018 and Decree No.150 /2018/ND-CP dated 7 November 2018 ("**Decree 72**");
- Decree No. 52/2013/ND-CP dated 16 May 2013 of the Government; as amended by Decree No. 08/2018/ND-CP dated 15 January 2018, on amendments to certain Decrees related to business conditions under state management of the Ministry of Industry and Trade and Decree No. 85/2021/ND-CP dated 25 September 2021 ("**Decree 52**");
- Decree No. 91/2020/ND-CP of the Government dated 14 August 2020 on anti-spam messages, emails and calls ("**Decree 91**");

- Decree No. 15/2020/ND-CP of the Government dated 3 February 2020 on penalties for administrative violations against regulations on postal services, telecommunications, radio frequencies, information technology and electronic transactions ("**Decree 15**");
- Decree No. 98/2020/ND-CP of the Government dated 26 August 2020 prescribing penalties for administrative violations against regulations on commerce, production and trade in counterfeit and prohibited goods, and protection of consumer rights; as amended by Decree No. 17/2022/ND-CP of the Government dated 31 January 2022 ("**Decree 98**");
- Circular No. 12/2022/TT-BTTTT of the Ministry of Information and Communications dated 12 August 2022 on guidelines for Decree 85 ("**Circular 12**");
- Circular No. 20/2017/TT-BTTTT dated 12 September 2017 of the Ministry of Information and Communications, providing for Regulations on coordinating and responding to information security incidents nationwide ("**Circular 20**");
- Circular No. 38/2016/TT-BTTTT dated 26 December 2016 of the Ministry of Information and Communications, detailing cross-border provision of public information ("**Circular 38**");
- Circular No. 24/2015/TT-BTTTT dated 18 August 2015 of the Ministry of Information and Communications, providing for the management and use of Internet resources, as latest amended and supplemented by Circular No. 21/2021/TT-BTTTT dated 8 December 2021 ("**Circular 25**");
- Decision No. 05/2017/QD-TTg of the Prime Minister dated 16 March 2017 on emergency response plans to ensure national cyber-information security ("**Decision 05**"); and
- Resolution No. 27/NQ-CP of the Government dated 7 March 2022 approving the Draft Personal Data Protection Decree ("**Resolution 27**").

Each aspect and each industry may have their respective regulating documents. In other words, applicability of legal documents will depend on the factual context of each case, e.g. businesses in the banking and finance, education, healthcare sectors may be subject to specialized data protection regulations, not to mention to regulations on employees’ personal information as provided in Labour Code 2019 (“**Labour Code**”).

The most important Vietnamese legal documents regulating data protection are the PDPD, the Cybersecurity Law and the Network Information Security Law. However, it is worth noting that, unlike cybersecurity laws in other jurisdictions that were inspired by the GDPR of the EU, the Cybersecurity Law of Vietnam shares similarities with China's Cybersecurity Law enacted in 2017. Such law focuses on providing the government with the ability to control the flow of information; meanwhile, the Network Information Security Law enforces data privacy rights for individual data subjects.

The PDPD took effect on 1 July 2023 without any transitional period (save in limited cases), and has affected all local and foreign enterprises which directly participate in or relate to personal data processing activities in Vietnam. The PDPD is the most comprehensive regulation governing the field of personal data protection. It sets out for the first time the key definitions of “personal data”, “sensitive personal data”, “data controller”, “data processor”, “personal data processing”, etc., which should be carefully examined in order to duly comply with the PDPD.

The PDPD is designed to have extraterritorial effect. The scope of the PDPD extends to foreign agencies, organizations and individuals directly involved in or related to the processing of personal data in Vietnam. Therefore, regardless of whether foreign entities have a local presence in Vietnam or not, to the extent that such entities are involved in the collection and processing of personal data of Vietnamese citizens, they are subject to the requirements of the PDPD.

Decree 53 took effect on 1 October 2022 and notably sets out the requirements relating to data localization and the establishment of branches / representative offices of foreign service providers, which will be discussed further below.

A Draft Decree on Sanctioning of Administrative Violations in the field of Cybersecurity ("**Draft Decree on Sanctioning**") was released by the Ministry of Public Security (“**MPS**”) for public consultation on 21 September 2021, notably including implementation guidelines for data localization requirements, together with a draft decree detailing the order of and procedures for the application of administrative sanctions against cybersecurity related violations and a draft decision of the Prime Minister promulgating a List of information systems important for national security, are being prepared by the MPS in coordination with other relevant ministries, ministerial-level agencies and bodies.

DEFINITIONS

Definition of personal data

Under the PDPD, personal data is defined as information on an electronic medium in the form of symbols, letters, numbers, photos, sounds, or the like that is associated with or helps to identify a specific individual. Information that helps to identify a specific individual is further clarified as information generated from an individual's activities that, when combined with other data and stored information, can identify a particular person.

Definition of sensitive personal data

The PDPD classifies personal data into two categories of “basic personal data” and “sensitive personal data”. Accordingly, basic personal data includes:

- surname, middle name, and birth name, alias (if any);
- date of birth, date of death or date of going missing;
- gender;
- place of birth, place of birth registration, permanent residence, current residence, hometown, contact address;
- nationality;
- personal image;
- phone number, ID card number, personal identification number, passport number, driver's license number, plate number, personal tax identification number, social insurance number; health insurance card number;
- marital status;
- family relationship information (parents, children);
- digital account information, personal data that reflects activities and activity history in cyberspace; and
- information associated with an individual or used to identify an individual other than sensitive personal data.

On the other hand, sensitive personal data includes:

- political and religious views;
- health conditions and personal information stated in health record, excluding information on blood type;
- information about racial or ethnic origin;
- information about genetic data relating to inherited or acquired genetic characteristics of each individual;
- information about physical or biological characteristics of each individual;
- information about criminals and criminal acts collected and stored by law enforcement agencies;
- information about sex life and sexual orientation of each individual;
- information on customers of credit institutions, foreign bank branches, intermediary payment service providers and other licensed institutions, including: customer identification as prescribed by law, accounts, deposits, deposited assets, transactions, organizations and individuals that are guarantors at credit institutions, bank branches, and intermediary payment service providers;
- personal location data identified via location services; and
- other specific personal data as specified by law as special and subject to necessary confidentiality measures.

Definition of Data Controller, Data Processor, Data Controller-Processor and Third Party

The PDPD also provides the definitions and roles of different stakeholders involved in the collection and processing of personal data with their respective obligations, notably:

- Data controller

A data controller is an organization or individual that decides the purposes and means of processing personal data. The controller is responsible for serving privacy notices to and obtaining consent from the data subjects, preparing and filing to the authority a Data Processing Impact Assessment (“**DPIA**”) and Cross-border Transfer Impact Assessment (“**TIA**”), notifying the authority of violations of regulations on personal data protection, ensuring and honouring the data subjects’ rights, etc.

- Data processor

A data processor is an organization or individual that processes data on behalf of the controller via a contract or agreement with the controller. Accordingly, the processor must receive and process personal data strictly in compliance with the contract or agreement with the controller. In particular, after the completion of the data processing / agreed purposes, the law requires the processor to delete and return all personal data to the controller. The processor is responsible for preparing and filing to the authority a processor’s DPIA and a TIA, notifying the controller of violations of regulations on personal data protection, etc.

- Data controller-processor

A data controller-processor is an organization or individual that jointly decides the purposes and means, and directly processes personal data. Consequently, the controller-processor must fully comply with both the responsibilities of the controller and the processor.

- Third party

A third party is defined as “an organization or individual other than the data subject, data controller or the data processor that is permitted to process personal data”.

Definition of Personal Data Processing

Under the PDPD, “personal data processing”, or “processing” is rather broad. It refers to one or multiple activities that impact personal data, including collection, recording, analysis, confirmation, storage, rectification, disclosure, combination, access, tracing, retrieval, encryption, decryption, copying, sharing, transmission, provision, transfer, deletion, destruction or other relevant activities. With such wide and open-ended definition of personal data processing, it appears that all types of activities related to personal data could be considered processing personal data and subject to the requirements prescribed by the PDPD.

NATIONAL DATA PROTECTION AUTHORITY

Vietnam does not have a single national data protection authority. Instead, the authority on State management of certain aspects of information and / or data protection has been given to a number of competent State authorities. To some extent, the key State competent authorities in charge of information and / or data protection would be the MPS, the Ministry of Information and Communications ("**MIC**") and the Vietnam Cybersecurity Emergency Response Teams / Coordination Center ("**VNCERT/CC**") directly managed by the Authority of Information Security ("**AIS**") under the MIC. Their key roles are particularly as follows:

- The MPS, particularly the Department for Cybersecurity and High-tech Crime Prevention and Fighting ("A05"), is responsible for supervision of processing of personal data and national cybersecurity, e.g. to request cyberspace service providers to (i) store data and establish branches or representative offices in Vietnam (if applicable), (ii) provide users' information for serving investigation into cybersecurity crime. The MPS has established and is managing and operating the National Portal on personal data protection; and is tasked to assess the sufficiency of personal data protection by relevant agencies, organizations and individuals;
- The MIC, particularly the AIS, is responsible for management of the provision of cyberspace services (e.g. social networks, online gaming, e-commerce, etc.), such as requesting cyberspace service providers to delete illegal data uploaded on their system/network; and
- VNCERT/CC acts as the National Coordination Center for response to cybersecurity incidents and information security testing.

In addition to the above, subject to each specific industry (e.g. banking and finance; education; healthcare; natural resources and environment; culture, sports and tourism; etc.), the State management authority in charge of such industry and its IT center shall be involved in relevant information system protection.

REGISTRATION

There is no requirement under current Vietnamese laws whereby such data controller of private sector is required to have it or its activities registered with the local authorities (e.g. MPS, MIC or VNCERT/CC), except in cases where:

- Foreign enterprises which provide services on telecom networks and on the Internet and other value-added services in cyberspace in Vietnam (“**cyberspace service providers**”) may need to have branches or representative offices in Vietnam (subject to specific guidance of the Government under Decree 53);
- Where organizations or individuals involved in cross-border public information provision activities rent digital information storage facilities within the territory of Vietnam so as to provide their services or are reported to provide public information to be used or accessed by at least 1 (one) million Internet users in Vietnam a month, they shall have the obligation to send a written notice to the MIC via post or email, informing the MIC of the following information:
    - In the case of an organization, registered name, transactional name, and name of the licensing country are required; in the case of an individual, name of such individual is required;
    - Main office address of an organization, permanent residence address and nationality of an individual owning an electronic information page and location of the main server system;
    - Principal contact agent of an overseas organization or individual and principal contact agent operated within the territory of Vietnam, including the following information such as name of an organization, individual, contact email address and telephone number.

However, data controllers and data processors who collect / process personal data of Vietnamese citizens and / or collect / process personal data in Vietnam are required to submit a DPIA and / or a TIA to the authority (i.e. the A05), as the case may be.

The DPIA must be prepared in a written form and be made available at all time for the inspection and evaluation by the A05. In addition, the controller / processor / controller-processor must send an original copy of the DPIA to the A05 according to a standard form (included in the PDPD) within 60 days from the date of the personal data processing. The A05 will then appraise the DPIA and request revision if it finds that the DPIA is incomplete. Any change to the DPIA’s contents must be submitted to the A05.

Please refer to the section of “Transfer” for details relating to the requirement on preparation and submission of the TIA.

DATA PROTECTION OFFICERS

When sensitive personal data is collected and processed, information on the Data Protection Department (“**DPD** ”) and Data Protection Officer (“**DPO**”) must be notified to the authority. In practice, the notification will be made by providing the information in the DPIA and the TIA dossiers submitted to the authority.

The PDPD does not set out any specific qualifications of the person eligible to be appointed as a DPO. In practice, the DPO should be an employee of the company, rather than an external counsel. However, if the company does not have any person suitable for taking the DPO position, the company may appoint an employee of its parent company and / or affiliated company within the same organization to take the DPO position for the company, if needed.

In addition, the appointment of a DPD / DPO must be made in the form of a written decision made by the company (i.e. a board resolution or a letter of appointment signed by the company's legal representative and affixed with the stamp of the company) and a copy of this written decision is required to be submitted alongside the DPIA / TIA dossiers.

COLLECTION & PROCESSING

According to Vietnamese laws, the solid legal basis for the processing of personal information (that means the performance of one or some acts of collecting, editing, utilizing, storing, providing, sharing or spreading personal information in cyberspace for commercial purpose) is a prior explicit consent given by the data subject. Consent requirements are among the most important regulations under the PDPD, and also among the most remarkable / novel changes brought about by the PDPD compared to the existing legal regime on data privacy.

Under the PDPD, the consent obtained from the data subjects must be clear, affirmative and in strict compliance with the consent form under the PDPD.

The PDPD sets out that consent must be voluntarily made based on the data subject's full understanding of (i) the purpose of the personal data processing; (ii) the type of personal data to be processed; (iii) the entities authorized to process personal data; (iv) the data subject's rights and obligations; and (v) the data to be processed that is sensitive personal data, if any. In addition, consent must be expressed clearly and specifically in writing, by voice, by ticking a consent box, by text message, by selecting consent technical settings, or via other actions which demonstrates the same. Moreover, consent must be expressed in a format that can be printed out or reproduced in writing, including in electronic or verifiable formats.

Importantly, the PDPD also explicitly points out that silence or non-response by the data subject is not construed as consent. Furthermore, consent must be made for a single purpose. That is to say, multiple purposes need to be demonstrated in a way that data subjects can give consent to one or more of them. Additionally, the data subjects may also opt to provide a partial or conditional consent.

However, the PDPD stpiulates that the processing of personal data could be carried out without consent in the following circumstances:

- In urgent cases where it is necessary to immediately process relevant personal data to protect the life or health of the data subject or others. The controller, processor, controller-processor and third party are responsible for proving such situation;
- Where the public disclosure of personal data is in accordance with the law;
- When the processing of data is performed by competent state agencies in the event of a state of emergency related to national defense, national security, social order and safety, major disaster, or dangerous epidemic; when there is a threat to security and national defense but not to the extent that a state of emergency must be declared; or when the processing is to prevent and combat riots and terrorism, crimes, and violations of the law;
- When the processing is to fulfill the contractual obligations of the data subject with relevant agencies, organizations, and individuals as prescribed by law; or
- When the processing is to serve the activities of state agencies prescribed by sector-specific laws.

In addition, the PDPD allows data subjects to withdraw their consent given. However, such consent withdrawal shall not affect the lawfulness of the processing to which consent was given before it was withdrawn. The withdrawal of consent shall be expressed in a format that can be printed and reproduced in writing, including in electronic or verifiable format.

In addition, the traders and organizations collecting and using consumers' personal information on E- commerce websites shall not require the consumers / subjects' prior consent in the following cases:

- Collecting personal information that has been publicized on E-commerce websites;
- Collecting personal information to sign or perform contract of sale and purchase of goods and services;
- Collecting personal information to calculate the price and charge of use of information, products and services on the network environment; or
- Collection of personal information for performing other obligations in accordance with the law.

TRANSFER

In general, if a data controller wishes to share, disclose or otherwise transfer an individual’s personal information to a third party (including group companies), the data controller they must inform the data subjects and obtain prior explicit consent from such data subjects. In particular, the traders or organizations collecting and using the consumer’s personal information on an E-commerce website must have specific mechanisms for the information subjects may choose the permission or refusal of using their personal information in the cases of using personal information to send advertisements and introduce products and other commercial information.

In cases of cross-border transfers, the PDPD defines cross-border personal data transfer as any activity involving the use of cyberspace, electronic equipment, electronic means or other forms to transfer personal data of Vietnamese citizens to a location outside Vietnam. The use of a location outside Vietnam to process Vietnamese citizens’ personal data is also considered cross-border transfer of personal data, including:

i. Organizations, enterprises or individuals transferring personal data of Vietnamese citizens to organizations, enterprises or management bodies located overseas for processing in accordance with the purposes consented by the data subjects;
ii. Processing of personal data of Vietnamese citizens by use of automated systems located outside of Vietnam by the controller, controller-processor or processor in accordance with the purposes consented by the data subjects.

Given the foregoing, the transfer of personal data to other companies which are located overseas or processing of personal data of Vietnamese citizens merely by servers located overseas, without any local presence in Vietnam, are both considered cross-border transfer of personal data and subject to relevant requirements of the PDPD, notably the preparation and submission of the TIA to the authority.

The TIA shall be made available at all times for the inspection and evaluation by the A05/the MPS. In addition, the transferor shall send one original copy of the TIA to the A05 according to a standard form issued under the PDPD within 60 days from the date of the personal data processing. The A05 will then appraise the TIA and request the transferor to revise the dossier in case it finds that the TIA is incomplete. Moreover, any change to the TIA’s contents must be submitted to the A05 within 10 days from the date of request.

In addition to the above requirements, it is worth noting that data localization could also be imposed on certain businesses providing services in Vietnam. The data localization requirements are provided in certain legal documents, e.g.:

- According to Circular 24, electronic general information pages and social networks as entities licensed in Vietnam must use at least one domain name “.vn” and store information in servers identified by IP addresses in Vietnam.
- The Cybersecurity Law requires that domestic or foreign cyberspace service providers carrying out activities of collecting, exploiting / using, analysing and processing data being personal information, data about service users' relationships and data generated by service users in Vietnam must store such data in Vietnam for a specified period to be stipulated by the Government. In particular, according to Article 26 of the Decree 53, domestic and foreign enterprises providing telecoms and online services to customers in Vietnam may be required to locally store certain customer-related data in Vietnam for a certain period prescribed by law if the authority alerts them that their services / online platforms have been used to commit violations of Vietnam’s laws but such online service providers fail to remedy the situation upon the request of the authority. According to the latest version of the Decree 53, while all domestic organizations providing telecoms services and online services to customers in Vietnam would be required to store their customer data in Vietnam, the foreign organizations which could be subject to the foregoing data localization requirements only include those engaging in the following 10 services: (i) telecommunications; (ii) data storage and sharing in cyberspace; (iii) supply of national or international domains to service users in Vietnam; (iv) E-commerce; (v) online payment; (vi) intermediary payment; (vii) transport connection via cyberspace; (viii) social networking and social media; (ix) online electronic games; and (x) providing, managing or operating other information in cyberspace in the form of messages, phone calls, video calls, email or online chats. Pursuant to Decree 53, only the following types of data is required to be stored in Vietnam:
    - Data on personal information of service users: i.e. data on information in the form of symbols, letters, numbers, images, sounds, or equivalent to identify an individual (“**Personal Data**”);
    - Data created by service users in Vietnam: i.e. data on information in the form of symbols, letters, numbers, images, sounds, or equivalent reflecting the process of participating, operating, and using cyberspace of service users and information on devices and network services used for connection with cyberspace in the territory of the Socialist Republic of Vietnam. It should be noted that the information under this category of data which is required to be stored in Vietnam only includes information on service account name, service usage time, credit card information, email address, IP addresses for the latest login and logout, registered phone number associated with account or data (“**Account Data**”); and
    - Data on the relationships of service users: i.e., data on information in the form of symbols, letters, numbers, images, sounds, or equivalences reflecting and identifying relationships of service users with other people in

cyberspace. Decree 53 further specifies that the information under this category of data which is required to be stored in Vietnam only includes information on friends and groups with which the service user connects or interacts in cyberspace (“**Relationship Data**”).

Moreover, foreign enterprises engaging in the abovementioned services are also required to establish branches or representative offices in Vietnam in case the authority alerts them that their services / online platforms have been used to commit violations of Vietnam’s laws but failed to remedy upon the request of the authority. The time for such establishment shall commence when the enterprises receive the request to do so until such enterprises terminate their operation in Vietnam or the prescribed services are no longer available in Vietnam.

SECURITY

Organizations must take necessary managerial or technical measures to ensure that the personal information shall not be lost, stolen, disclosed, modified or destroyed. Remedial measures must be taken immediately if personal information is being or is likely to be disclosed or destroyed.

Indeed, generally, the data controller shall classify information based on its secrecy in order to take appropriate protection measures; and agencies and organizations that use classified and unclassified information in activities within their fields have to develop regulations and procedures for processing information, and determine contents and methods of recording authorized accesses to classified information, in which:

- Personal information protection policies to be developed and published by traders and organizations collecting and using the consumers’ personal information on E-commerce websites must provide the purpose of collection; scope of use; storage period; organizations and persons authorized to access to such personal information; address of data controller, including way of contact for the consumers to ask about the collection and processing information related to them; methods and tools for data subjects to access and modify their personal information on the E-commerce system of the data controller;
- The above contents must be clearly displayed for the consumers before or at the time of information collecting. The language is Vietnamese. The contents are clear and understandable. The font size of the text is at least 12. The paper background and ink colour used in the terms must contrast;
- If the information collection is done through E-commerce website of the data controller, the personal information protection policies must be made public in a conspicuous place on the website; and
- The traders, organizations or individuals that own E-commerce websites with online payment functions must publish on their website policies on security of customer’s payment information.

Under the PDPD, the data controller and processor shall implement the following personal data protection measures:

a. General personal data protection measures, including:
   i. Management measures adopted by an organization or individual related to processing of personal data;
   ii. Technical measures adopted by an organization or individual related to processing of personal data;
   iii. Measures adopted by a competent authority according to regulations in the PDPD and relevant law;
   iv. Investigation and procedure measures adopted by a competent authority;
   v. Other measures as prescribed by law.
b. Data protection measures applicable to the processing of basic personal data, including:
   i. Formulation and promulgation of regulations on personal data protection, which specify tasks to be performed in accordance with the PDPD;
   ii. Encouragement of application of standards of personal data protection in conformity with fields, industries and activities related to the processing of personal data;
   iii. Cybersecurity inspection for systems, means and equipment for processing of personal data before processing, permanent deletion or destruction of devices containing personal data.

c. Data protection measures applicable to the processing of sensitive personal data, including: appointment of a department with the function of protecting personal data (i.e. DPD) and personnel in charge of protection of personal data (i.e. head of the DPD (i.e. DPO)), and notification about the establishment of the DPD and the appointment of the DPO to the A05;
d. Notification to the data subject about the sensitive nature of the personal data to be processed; and the processing of such sensitive person.

BREACH NOTIFICATION

The laws of Vietnam introduced a general requirement for the reporting and notification of actual or suspected personal information security incidents. A data breach reporting / notification requirement in Vietnam will be triggered if the data incident falls within any of the following criteria:

Criterion 1. The affected data system is located in Vietnam.

Criterion 2. The services provided to customers in Vietnam fall under the categories of Regulated Services, including (1) telecommunication services; (2) data storage and sharing in cyberspace; (3) services providing national or international domain names to service users in Vietnam; (4) e-commerce; (5) online payment; (6) payment intermediary; (7) connecting transportation in cyberspace; (8) social networks and social media; (9) online games; and (10) other services that provide, manage and operate information in cyberspace in the form of messages, voice calls, video calls, email, or online chatting.

Criterion 3. The incident causes “significant loss” to the legitimate rights and interests of the affected Vietnamese persons.

Where there is a data security incident, organizations must promptly take relevant measures to mitigate and notify relevant data subjects and / or relevant competent State authorities, as the case may be, in a timely manner, e.g. 5 days after detection of the security incident, and must provide an update on the incident status when it is completely resolved. Affected organizations and individuals must be notified of the data incident if the incidents fall under Criterion 2 or Criterion 3.

In the case of an incident under Criteria 1 that is beyond the control of the organization, the operator of the information system must immediately prepare an initial report on the incident to report such incident to the relevant agencies and a final report on response to the incident within five days after finishing responding to the incident. Moreover, if the information system of a trader, organization or individual engaged in e-commerce is attacked causing risk of loss of consumer’s information, the data controller must notify the authorities within 24 hours after the detection of incident.

Normally, the data controller would be required to give relevant notifications to the following State authorities:

- Local police agency (i.e. Police Department of Cybersecurity and High-Tech Crime Prevention and Fighting under the MPS with regard to offshore service providers, provincial police department where the head office of data controller is located); and
- VNCERT/CC directly managed by the AIS under the MIC.

Criterion 4: The PDPD sets out a new reporting requirement that upon detection of any violation against regulations on personal data protection (which can be interpreted to include data breach incidents), the controller / controller-processor shall notify the A05 within 72 hours of the occurrence of such violation. The reason for late notification, if any, must be provided.

The information to be notified will include:

i. Description of the nature of the violation, including: time, place, violation, organization, individual, types of personal data and the amount of relevant data;

ii. Contact details of the employee(s) assigned to protect the data or organizations or individuals that are responsible for protecting personal data;
iii. Description of consequences and damage that may occur;
iv. Description of measures for handling and minimizing the harm caused by the violation.

If the abovementioned contents cannot be fully notified, the notification may be made in multiple stages. Thereafter, the controller / controller-processor shall prepare written minutes confirming the occurrence of the violation of the regulations on personal data protection, and coordinate with the A05 to handle the violation. In practice, as the 72-hour timeframe is very tight, more often than not, data controllers find it very challenging to comply with this timeframe. To the best of our knowledge, the regulator has not yet penalized any data controllers that file the report, but failed to meet the deadline.

In addition to the four criteria mentioned above, there are also data breach notification requirements imposed by sector-specific laws / regulation, such as laws / regulations governing financial services, e-commerce services, etc.

ENFORCEMENT

Subject to specific data protection laws and the regulations breached, the sanctions in relation to data protection breaches are scattered across various different laws and regulations. In general, amongst others, the major type of sanction would be administrative penalty. For example, failure to obtain prior consent of the data subjects on collection, processing and use of their information shall be subject to a monetary fine varying from VND 10 million to VND 20 million. In serious cases, according to the Criminal Code, any person who commits illegal use of information on the computer or telecommunications network may be liable to a monetary fine varying from VND 30 million to VND 1 billion or face a penalty of up to 3 years' community sentence or 6 months – 7 years' imprisonment; and the offender might also be liable to a monetary fine varying from VND 20 million to VND 200 million or prohibited from holding certain positions or doing certain jobs for 1 – 5 years.

As of early 2024, the MPS is preparing to promulgate the Draft Decree on Sanctioning. Once this decree takes effect, the MPS will have a basis to start imposing sanctions on non-compliance with the requirements under the PDPD.

This Draft Decree on Sanctioning was first released for public comments in September 2021, and its updated version was released to the public for the second round of consultation on 31 May 2023. The official Decree on Sanctioning is expected to be adopted by the middle of 2024.

Violators of the PDPD’s regulations, depending on the severity of their violations, may be warned, disciplined, or face administrative penalties or criminal prosecution. Generally, for PDPD-associated violations, the Draft Decree on Sanctioning has proposed a monetary fine of up to VND 1 billion (approx. USD 42,500). Additional penalties, applicable to certain violations, include: (i) deprivation of the right to use licenses for business lines requiring personal data collection; (ii) confiscation of exhibits and means of administrative violations. Remedial measures include: (i) 1-3 months of forcible suspension of processing personal data; (ii) forcible destruction or unrecoverable deletion of personal data; (iii) forcible return of illegal profits obtained from the violations; (iv) public apology; (v) forcible implementation of personal data processing notification measures; (vi) forcible personal data provision; (vii) forcible request to allow personal data correction; (viii) forcible implementation of personal data protection measures.

Notably, under the Draft Decree on Sanctioning, a penalty of up to 5% of the violating enterprise’s turnover of the immediately preceding fiscal year in the Vietnamese market applies to:

a. disclosing and misplacing the personal data or cross-border transfer of 5 million data subjects who are Vietnamese citizens; and
b. a second violation of the regulations on:
    - personal data protection in marketing and advertising activities; and
    - illegal collection, transfer, purchase and selling of personal data.

In addition, the MPS has set up a National Portal of Personal Data Protection to receive reports on violation of the PDPD. Once this portal is fully operational, companies are expected to be more vulnerable to inspection actions in this area, as the portal would enable data subjects like employees or clients to easily report on companies’ acts of non-compliance with the PDPD and breach of their personal data.

ELECTRONIC MARKETING

According to Vietnam’s new anti-spam regulation (i.e. Decree No. 91/2020/ND-CP on anti-spam text messages, emails and calls), advertisements by text message, email and call may only be sent or made in compliance with specific requirements, notably including:

- it is prohibited to send advertising messages or make advertising calls to phone numbers on the Do-Not-Call Register;
- for phone numbers not included in the Do-Not-Call Register, only one initial advertising registration message (i.e. a message inquiring whether the user would like to receive advertising communications from the advertiser) is allowed;
- if the user refuses to receive advertising messages after receiving the initial advertising registration message, no further advertising message is allowed;
- immediately after receiving a refusal request from a user, the advertiser must terminate providing advertising messages, email or calls to such user;
- no more than three advertising messages / three advertising emails / one advertising call per day may be sent or made to the same user;
- advertising messages are only allowed from 7 a.m. to 10 p.m.; advertising calls are only allowed from 8 a.m. to 5 p.m.; and
- advertising contents must comply with advertising laws.

Once again, the traders or organizations collecting and using the consumers’ personal information on E-commerce websites must have a specific mechanism for the information subjects to choose the permission or refusal of using their personal information in the cases of using personal information to send advertisements and introduce products and other commercial information.

Additionally, the organization shall not be allowed to hide their names or use unlawfully the name of others when sending advertisements via e-mail or text message. Specific information must be stated in each electronic message: for example, information about the advertiser and the advertising service provider, opt-out function (refusing acceptance of advertisements), and a label identifying “QC” or “ADV” [QC means Adv. in Vietnamese].

With regard to the method of advertising into Vietnam (i.e. to target Vietnam-based recipients), foreign organizations which do not operate in Vietnam (i.e. do not have commercial presence in Vietnam) but wish to advertise their products, goods, services and operation in Vietnam, are required to hire a Vietnam-based advertising service provider (a company with business lines of provision of advertisement) to conduct relevant advertising activities.

ONLINE PRIVACY

To some extent, by assisting in tracking the information on a specific person, the cookies and location data could be deemed as tools preinstalled on the users’ computers for collecting, storing and using their personal information, which may disclose his / her private life, e.g. hobbies, favourite websites and locations usually visited by him / her.

As such, it is currently understood that all rules on data protection are applicable to cookies as well as location data. For example, cyberspace service provider must seek for users’ prior acceptance before some certain technologies (e.g. cookies, positioning service) are activated.

KEY CONTACTS

Tilleke & Gibbins
www.tilleke.com/

Waewpen Piemwichai
Counsel
Tilleke & Gibbins
T +84 24 3772 6688
waewpen.p@tilleke.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ZAMBIA

Last modified 23 December 2021

LAW

Data Protection Act No. 3 of 2021 (the **“DPA"**).

DEFINITIONS

Definition of Personal Data

Data which relates to an individual who can be directly or indirectly identified from that data which includes a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Definition of Sensitive Personal Data

Personal data which by its nature may be used to suppress the data subject’s fundamental rights and freedoms and includes:

- the race, marital status, ethnic origin or sex of a data subject;
- genetic data and biometric data;
- child abuse data;
- a data subject’s political opinions;
- a data subject’s religious beliefs or other beliefs of a similar nature;
- whether a data subject is a member of a trade union; or
- a data subject’s physical or mental health, or physical or mental condition.

NATIONAL DATA PROTECTION AUTHORITY

The Office of the Data Protection Commissioner.

REGISTRATION

A person shall not control or process personal data without registering as a data controller or a data processor under the DPA.

DATA PROTECTION OFFICERS

Data controllers and data processors are required to appoint a data protection officer in line with the guidelines issued by the Data Protection Commissioner.

COLLECTION & PROCESSING

In order to collect or process personal data consent of the data subject must be obtained. A data subject may consent to such processing in writing. Prior to giving such consent, the data subject must be informed of the data subject’s right to withdraw the consent. Furthermore except as expressly provided in the DPA, a data controller is required to collect personal data directly from the data subject. The DPA provides additional rules in respect of collection and processing of personal data as set out below.

A data controller or data processor shall ensure that personal data is:

- processed lawfully, fairly and transparently;
- collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- accurate and where necessary, kept up to date, with every reasonable step taken to ensure that any inaccurate personal data is erased or rectified without delay;
- stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;
- processed in accordance with the rights of a data subject; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against any loss, destruction or damage, using appropriate technical or organisational measures.

Subject to the other provisions of the DPA, a data controller may process personal data where:

- the data subject has given consent to the processing of that data subject’s personal data;
- the processing is necessary
    - for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
    - for compliance with a legal obligation to which the data controller is subject;
    - in order to protect the vital interests of the data subject or of another natural person;
    - for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
    - for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interest or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child; or
- the processing relates to personal data which is manifestly made public by the data subject.

A person shall not process sensitive personal data, unless:

- processing is necessary for the establishment, exercise or defence of a legal claim or whenever a court is exercising a judicial function;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services; or
- processing is necessary for reasons of public interest.

Where a data subject is a child or a vulnerable person, that data subject’s right may be exercised by that data subject’s parents, legal guardian or a person exercising parental responsibility as the case may be. A data controller shall not process a child’s or vulnerable person’s personal data unless consent is given by the child’s or vulnerable person’s parent, legal guardian or a person exercising parental responsibility. A data controller shall, where the personal data of a child or a vulnerable person is involved, make every reasonable effort to verify that consent has been given or authorised, taking into account available technology. A data controller shall incorporate appropriate mechanisms for age verification and parental consent in the processing of personal data of a child.

TRANSFER

Transfer of personal data and sensitive personal data is subject to certain restrictions under the DPA. The DPA provides that personal data must be processed and stored on a server or data centre located in the Republic. The Minister may however prescribe categories of personal data that may be stored outside the Republic. The powers of the Minister notwithstanding, sensitive personal data must be processed and stored in a server or data centre located in the Republic.

Furthermore, the DPA provides that Personal data other than personal data categorised by the Minister may be transferred outside the Republic where:

- the data subject has consented and
  - the transfer is made subject to standard contracts or intragroup schemes that have been approved by the Data Protection Commissioner; or
  - the Minister, has prescribed that transfers outside the Republic is permissible; or
- the Data Protection Commissioner approves a particular transfer or set of transfers as permissible due to a situation of necessity.

Additional exceptions for the transfer of personal data outside the Republic are provided for, including:

- in case of an emergency, to a particular person or entity engaged in the provision of health services or emergency services;
- where the data subject has explicitly consented to that transfer of sensitive personal data; and
- to a particular international organisation or country which complies with the DPA, where the Data Protection Commissioner is satisfied that the transfer or class of transfers is necessary for any class of data controllers or data subjects and does not hamper the effective enforcement of the DPA.

SECURITY

A data controller or data processor is required to provide guarantees regarding the technical and organisational security measures employed to protect the personal data associated with the processing undertaken and ensure strict adherence to such measures.

A data controller or the data processor is further required to, having regard to the nature, scope and purpose of processing personal data undertaken, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement appropriate security safeguards including:

- maintaining integrity of personal data using methods including pseudonymisation and encryption;
- ensuring ongoing confidentiality, integrity and implementation of measures necessary to protect the integrity of personal data;
- measures necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data; and
- implementation of appropriate data protection policies.

A data controller and data processor is also required to undertake a periodic review of security safeguard in accordance with guidelines issued by the Data Protection Commissioner.

BREACH NOTIFICATION

A data controller shall notify the Data Protection Commissioner within twenty-four hours of any security breach affecting personal data processed.

A data processor shall notify the data controller, as soon as practicable of any security breach affecting personal data processed on behalf of the data controller.

A data controller or data processor shall notify the data subject, as soon as practicable of any security breach affecting personal data processed.

Mandatory breach notification

A data controller shall notify the Data Protection Commissioner within twenty-four hours of any security breach affecting personal data processed.

A data processor shall notify the data controller, as soon as practicable of any security breach affecting personal data processed on behalf of the data controller.

A data controller or data processor shall notify the data subject, as soon as practicable of any security breach affecting personal data processed.

ENFORCEMENT

The DPA sets out various penalties for offences prescribed thereunder. For example in respect of offences relating to the breach of the principles and rules relating to the processing of personal data, the penalty upon conviction is a fine not exceeding one hundred million penalty units[1] or two percent of annual turnover of the preceding financial year whichever is higher where the offence is committed by a corporate body.

Given that the DPA is a new piece of legislation, at the date of this update, we are not aware of any enforcement action taken by the Regulator.

---

[1] ZMW30,000,000 (at today’s exchange rate of US$1-ZMW16.37 approx. US$1,832,620.65)

ELECTRONIC MARKETING

Electronic marketing is governed by the Electronic Communications and Transactions Act No. 4 of 2021 (the “ ECTA’). The ECTA provides that a person marketing by means of electronic communication shall provide the addressee with:

- the person’s identity and contact details including its registered office and place of business, email, contact and customer service number;
- a valid and operational opt out facility from receiving similar communications in future;
- the identifying particulars of the source from which the originator obtained the addressee’s personal information; and
- applicable privacy and other user policies.

The ECTA also places restrictions in respect of unsolicited commercial communications to a consumer. The ECTA provides that a person may send one unsolicited commercial communication to a consumer, such commercial message can only be sent where the opt in requirement is met.

The ECTA further provides that an originator who sends unsolicited commercial communications to an addressee who has opted-out from receiving any further electronic communications from the originator through the originator’s opt out facility, commits an offence.

ONLINE PRIVACY

The ECTA provides that a service provider is not liable for any damage incurred by a person if the service provider refers or links users to a web page containing an infringing data message or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink, and where the service provider:

- does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of that person;

- is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent;
- does not receive a financial benefit directly attributable to the infringing activity; and
- removes, or disables access to, the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to that data message, infringes the rights of a person.

KEY CONTACTS

Chibesakunda & Co.
www.dlapiperafrica.com/zambia/

Louise De-Assis Chilepa
Head of Banking & Finance
T +260 211 366400
louise.chilepa@cco.co.zm

Mwamba Chibesakunda
Associate
T +260 211 366400
mwamba.chibesakunda@cco.co.zm

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

ZIMBABWE

Last modified 22 January 2024

LAW

Access to Information and Protection of Privacy Act (Chapter 10:27);

Banking Act (Chapter 24:20);

Courts and Adjudicating Authorities (Publicity Restrictions) Act (Chapter 07:04);

Consumer Protection Act (Chapter 14:44);

Census and Statistics Act (Chapter 10:29);

Cyber and Data Protection Act (Chapter 12:07);

Interception of Communications Act (Chapter 11:20); and,

National Registration Act (Chapter 10:17);

Communication Technology (“ICT Policy”).

DEFINITIONS

Definition of personal data

The Access to Information and Protection of Privacy Act defines personal information as recorded information about an identifiable person which includes:

- The person's name, address, or telephone number;
- The person's race, national or ethnic origin, religious or political beliefs or associations;
- The person's age, sex, sexual orientation, marital status, or family status;
- An identifying number, symbol or other particulars assigned to that person;
- Fingerprints, blood type or inheritable characteristics;
- Information about a person's healthcare history, including a physical or mental disability;
- Information about educational, financial, criminal or employment history;
- A third party's opinions about the individual;
- The individual's personal views or opinions (except if they are about someone else); and,
- Personal correspondence with home or family.

Definition of sensitive personal data

There is no law that defines Sensitive **Personal** Data. However, in terms of the Data Protection Act **sensitive data** refers to:

- information or any opinion about an individual which reveals or contains the following:
  - racial or ethnic origin;
  - political opinions;
  - membership of a political association;
  - religious beliefs or affiliations;
  - philosophical beliefs;
  - membership of a professional or trade association;
  - membership of a trade union;
  - sex life;
  - criminal educational, financial or employment history;
  - gender, age, marital status, or family status;
- health information about an individual;
- genetic information about an individual; or
- any information which may be considered as presenting a major risk to the rights of the data subject;

NATIONAL DATA PROTECTION AUTHORITY

In terms of the Data Protection Act, the Postal and Telecommunication Regulatory Authority established in terms of section 5 of the Postal and Telecommunications Act [Chapter 12:05]; is the recognised National Data Protection Authority. The Authority has the responsibility to promote and enforce the fair processing of personal data and advise the Minister of Information Communication Technology on matters relating to privacy rights. The Authority is mandated to conduct inquiries and investigations either on its own accord or on the request of any interested person in relation to data protection rights.

Under the recently enacted Draft Protection Act, a data protection officer must be appointed to ensure the compliance with all obligations provided for in the Data Protection Act.

The Zimbabwe Media Commission's mandate does the following:

- Ensures that the people of Zimbabwe have equitable and wide access to information;
- Comments on the implications of proposed legislation or programs of public bodies on access to information and protection of privacy; and,
- Comments on the implications of automated systems for collection, storage, analysis, or transfer of information or for the access to information or protection of privacy.

The Revised ICT Policy proposes the establishment of a quasi-government entity to monitor Internet traffic. It states that all Internet gateways and infrastructure will be controlled by a single company, while a National Data Centre to support both public and high security services and information will be established.

REGISTRATION

There is no law that requires the registration of databases.

DATA PROTECTION OFFICERS

In terms of the Data Protection Act, a Data Protection Officer refers to any individual appointed by the data controller and is charged with ensuring, in an independent manner, compliance with the obligations provided for in this Act.

COLLECTION & PROCESSING

There are no specific provisions for the collectors of personal data to obtain the prior approval of data subjects for the processing of their personal data. However, when collecting data the controller or the controller’s representative shall provide the data subject with at least the following information:

- the name and address of the controller and of his or her representative, if any;

- the purposes of the processing;
- the existence of the right to object, by request and free of charge, to the intended processing of data relating to him or her, if it is obtained for the purposes of direct marketing;
- whether compliance with the request for information is compulsory or not, as well as what the consequences of the failure to comply are;
- taking into account the specific circumstances in which the data is collected, any supporting information, as necessary to ensure fair processing for the data subject, such as:
    - the recipients or categories of recipients of the data;
    - whether it is compulsory to reply, and what the possible consequences of the failure to reply are;
    - the existence of the right to access and rectify the data relating to him or her except where such additional information, taking into account the specific circumstances in which the data is collected is not necessary to guarantee accurate processing.
- other information dependent on the specific nature of the processing, as specified by the Authority.

For purposes of processing the information Section 13 of the Data Protection Act is quite instructive. In terms of that Section every data controller or data processor shall ensure that personal information is:

- processed in accordance with the right to privacy of the data subject;
- processed lawfully, fairly and in a transparent manner in relation to any data subject;
- collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;

The Census and Statistics Act contains provisions which restrict the use and disclosure of information obtained during the conducting of a census exercise. Under this Act, authorities are able to collect, compile, analyse, and abstract statistical information relating to any of the following:

- Commercial
- Industrial
- Agricultural
- Mining
- Social
- Economic
- General activities and conditions of the inhabitants of Zimbabwe and to publish such statistical information

TRANSFER

The transfer of data to any other jurisdiction is governed in terms of Part VII of the Data Protection Act under section 28 and 29.

In terms of Section 28 of the Data Protection Act:

- a data controller may not transfer personal information about a data subject to a third party who is in a foreign country unless an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the
  data is transferred solely to allow tasks covered by the competence of the controller to be carried out.

- The adequacy of the level of protection afforded by the third country or international organisation in question shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; with particular consideration being given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the recipient third country or recipient international organisation, the laws relating to data protection in force in the third country or international organisation in question and the professional rules and security measures which are complied with in that third country or international organisation.

- The Authority shall lay down the categories of processing operations for which and the circumstances in which the transfer of data to countries outside the Republic of Zimbabwe is not authorised.

- The Minister responsible for the Cyber security and Monitoring Centre in consultation with the Minister, may give directions on how to implement this section with respect to transfer of personal information outside of Zimbabwe.

SECURITY

Section 18 of the Data Protection Act provides guidelines for the protection of data. It states that to safeguard the security, integrity and confidentiality of the data, the controller or his or her representative, if any, or the processor, shall take the appropriate technical and organisational measures that are necessary to protect data from negligent or unauthorised destruction, negligent loss, unauthorised alteration, or access and any other unauthorised processing of the data.

Further the Section also provides that the Data Protection Authority may issue appropriate standards relating to information security for all or certain categories of processing. Since the enactment of this Act the Data Protection Authority is still to issue any appropriate standards.

The Revised ICT Policy states that there will be development, implementation and promotion of appropriate security and legal systems for e-commerce, including issues related to cybersecurity, data protection and e-transactions. The Policy states that the following laws will be enacted to cater for intellectual property rights, data protection and security, freedom of access to information, computer related and cybercrime laws:

- data protection and privacy
- intellectual property protection and copyright
- consumer protection and
- child online protection.

BREACH NOTIFICATION

Breach notification

Section 19 of the Data Protection Act places a duty on the data controller to notify the Authority “within twenty-four (24) hours of any security breach affecting data he or she processes.

Mandatory breach notification

Section 19 of the Data Protection Act uses the word “**shall**” which makes it mandatory to notify the Authority within twenty-four (24) hours.

ENFORCEMENT

The Constitution mandates the Human Rights Commission (HRC) to enforce a citizen's human rights where they have been violated. The right to privacy, including the right not to have the privacy of one's communication infringed, is a basic human right and, thus, falls within the purview of the HRC. However, the Cyber Security and Monitoring of Interceptions of Communications Centre (CSMICC), established by the Interception of Communications Act, is mandated to, among other things, monitor communications made over telecommunications, radio communications and postal systems and to give technical advice to service providers. The mandate of the CSMICC does not preclude it from monitoring computer-based data for the purposes of enforcing an individual's right to privacy where it is found that such right has been infringed.

Further, the CSMICC also has the duty to oversee the enforcement of the Act to ensure that it is enforced reasonably and with due regard to fundamental human rights and freedoms.

ELECTRONIC MARKETING

Zimbabwe recently enacted the Consumer Protection Act (Chapter 14:44) which has introduced several measures aimed at protecting consumers from unfair trade practices.

The Consumer Protection Act does not make specific reference to electronic marketing; however, it provides certain guidelines around electronic transactions, Information to be provided by the service provider, a cooling-off period in electronic transactions and unsolicited goods, services, or communications.

ONLINE PRIVACY

There is currently no specific online privacy legislation.

KEY CONTACTS

Manokore Attorneys
www.dlapiperafrica.com/en/zimbabwe/

Farai Nyabereka
Partner
Manokore Attorneys
T +263 4 746 787
fnyabereka@manokore.com

Steve Chikengezha
Associate
Manokore Attorneys
T +263 773 376 633
schikengezha@manokore.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.