<table>
<thead>
<tr>
<th>Country</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Angola</td>
<td>8</td>
</tr>
<tr>
<td>Argentina</td>
<td>14</td>
</tr>
<tr>
<td>Australia</td>
<td>19</td>
</tr>
<tr>
<td>Austria</td>
<td>25</td>
</tr>
<tr>
<td>Bahrain</td>
<td>39</td>
</tr>
<tr>
<td>Belarus</td>
<td>44</td>
</tr>
<tr>
<td>Belgium</td>
<td>48</td>
</tr>
<tr>
<td>Bermuda</td>
<td>63</td>
</tr>
<tr>
<td>Bosnia and Herzegovina</td>
<td>66</td>
</tr>
<tr>
<td>British Virgin Islands</td>
<td>71</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>74</td>
</tr>
<tr>
<td>Canada</td>
<td>89</td>
</tr>
<tr>
<td>Cape Verde</td>
<td>96</td>
</tr>
<tr>
<td>Cayman Islands</td>
<td>100</td>
</tr>
<tr>
<td>China</td>
<td>103</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>111</td>
</tr>
<tr>
<td>Croatia</td>
<td>114</td>
</tr>
<tr>
<td>Cyprus</td>
<td>126</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>139</td>
</tr>
<tr>
<td>Denmark</td>
<td>149</td>
</tr>
<tr>
<td>Egypt</td>
<td>157</td>
</tr>
<tr>
<td>Estonia</td>
<td>160</td>
</tr>
<tr>
<td>Finland</td>
<td>173</td>
</tr>
<tr>
<td>France</td>
<td>189</td>
</tr>
<tr>
<td>Germany</td>
<td>200</td>
</tr>
<tr>
<td>Ghana</td>
<td>215</td>
</tr>
<tr>
<td>Gibraltar</td>
<td>219</td>
</tr>
<tr>
<td>Greece</td>
<td>224</td>
</tr>
<tr>
<td>Guernsey</td>
<td>241</td>
</tr>
<tr>
<td>Honduras</td>
<td>247</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>251</td>
</tr>
<tr>
<td>Hungary</td>
<td>256</td>
</tr>
<tr>
<td>Iceland</td>
<td>267</td>
</tr>
<tr>
<td>India</td>
<td>279</td>
</tr>
<tr>
<td>Indonesia</td>
<td>284</td>
</tr>
<tr>
<td>Ireland</td>
<td>291</td>
</tr>
<tr>
<td>Israel</td>
<td>304</td>
</tr>
<tr>
<td>Italy</td>
<td>309</td>
</tr>
<tr>
<td>Japan</td>
<td>320</td>
</tr>
<tr>
<td>Jersey</td>
<td>326</td>
</tr>
<tr>
<td>Latvia</td>
<td>330</td>
</tr>
<tr>
<td>Lesotho</td>
<td>342</td>
</tr>
<tr>
<td>Lithuania</td>
<td>347</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>361</td>
</tr>
<tr>
<td>Macau</td>
<td>373</td>
</tr>
<tr>
<td>Macedonia</td>
<td>377</td>
</tr>
<tr>
<td>Madagascar</td>
<td>381</td>
</tr>
<tr>
<td>Malaysia</td>
<td>385</td>
</tr>
<tr>
<td>Malta</td>
<td>391</td>
</tr>
<tr>
<td>Mauritius</td>
<td>406</td>
</tr>
<tr>
<td>Country</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Mexico</td>
<td>413</td>
</tr>
<tr>
<td>Monaco</td>
<td>419</td>
</tr>
<tr>
<td>Montenegro</td>
<td>423</td>
</tr>
<tr>
<td>Morocco</td>
<td>428</td>
</tr>
<tr>
<td>Netherlands</td>
<td>432</td>
</tr>
<tr>
<td>New Zealand</td>
<td>442</td>
</tr>
<tr>
<td>Nigeria</td>
<td>448</td>
</tr>
<tr>
<td>Norway</td>
<td>455</td>
</tr>
<tr>
<td>Pakistan</td>
<td>465</td>
</tr>
<tr>
<td>Panama</td>
<td>468</td>
</tr>
<tr>
<td>Philippines</td>
<td>472</td>
</tr>
<tr>
<td>Poland</td>
<td>479</td>
</tr>
<tr>
<td>Portugal</td>
<td>495</td>
</tr>
<tr>
<td>Qatar</td>
<td>509</td>
</tr>
<tr>
<td>Romania</td>
<td>513</td>
</tr>
<tr>
<td>Russia</td>
<td>527</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>532</td>
</tr>
<tr>
<td>Serbia</td>
<td>535</td>
</tr>
<tr>
<td>Seychelles</td>
<td>539</td>
</tr>
<tr>
<td>Singapore</td>
<td>544</td>
</tr>
<tr>
<td>Slovak Republic</td>
<td>549</td>
</tr>
<tr>
<td>Slovenia</td>
<td>556</td>
</tr>
<tr>
<td>South Africa</td>
<td>566</td>
</tr>
<tr>
<td>South Korea</td>
<td>571</td>
</tr>
<tr>
<td>Spain</td>
<td>580</td>
</tr>
<tr>
<td>Sweden</td>
<td>590</td>
</tr>
<tr>
<td>Switzerland</td>
<td>601</td>
</tr>
<tr>
<td>Taiwan</td>
<td>608</td>
</tr>
<tr>
<td>Thailand</td>
<td>612</td>
</tr>
<tr>
<td>Trinidad and Tobago</td>
<td>615</td>
</tr>
<tr>
<td>Turkey</td>
<td>620</td>
</tr>
<tr>
<td>UAE - Dubai (DIFC)</td>
<td>626</td>
</tr>
<tr>
<td>UAE - General</td>
<td>633</td>
</tr>
<tr>
<td>Ukraine</td>
<td>639</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>646</td>
</tr>
<tr>
<td>United States</td>
<td>660</td>
</tr>
<tr>
<td>Uruguay</td>
<td>665</td>
</tr>
<tr>
<td>Zimbabwe</td>
<td>668</td>
</tr>
</tbody>
</table>
ABSTRACT

More than ever it is crucial that organisations manage and safeguard personal information and address their risks and legal responsibilities in relation to processing personal data, to address the growing thicket of applicable data protection legislation.

A well constructed and comprehensive compliance program can solve these competing interests and is an important risk management tool.

This handbook sets out an overview of the key privacy and data protection laws and regulations across nearly 100 different jurisdictions and offers a primer to businesses as they consider this complex and increasingly important area of compliance.

DLA Piper’s global data protection and privacy team has the deep experience and international reach to help global businesses develop and implement practical compliance solutions to the myriad data protection laws that apply to global businesses.

INTRODUCTION

Welcome to DLA Piper’s Data Protection Laws of the World Handbook. We launched the first edition of the handbook in 2012, and following such a positive response have been updating it annually ever since.

We continue to witness a period of unprecedented activity in the development of data protection regulation around the world which will have a profound impact on the way in which global businesses are required to approach the collection and management of personal information.

These changes are being driven largely by cultural and trade considerations and by a struggle to keep pace with emerging technology and online business methods.

Should you require further guidance, please do not hesitate to contact us at dataprivacy@dlapiper.com.

DATA PRIVACY SCOREBOX

You may also be interested in our Data Privacy Scorebox, a tool to help you assess your data protection strategy. It requires completing a survey covering 12 areas of data privacy, such as storage of data, use of data, and customers’ rights. Once completed, a report summarising your organisation’s alignment with key global principles of data protection is produced. The report includes a visual summary of the strengths and weaknesses of your data protection strategy, a practical action point check list, as well as peer benchmarking data.

To access the Scorebox, please visit www.dlapiper.com/dataprotection.

CYBERTRAK

We are pleased to introduce CyberTrak, an innovative online cybersecurity tool featuring information on cybersecurity-related mandates in 23 key markets around the world. CyberTrak is the inaugural product of Blue Edge Lab®.

CyberTrak provides multinational companies instant online access to critical information about cybersecurity-related laws, regulations and generally accepted standards in 23 key markets in the Americas, Asia-Pacific, Europe and the Middle East and in four highly regulated sectors in the US. It also provides brief summaries of requirements, as well as an assessment on enforcement risk and the degree of activity triggering the requirement.

Cybersecurity laws and regulations are evolving rapidly around the world. Companies battling ever more sophisticated cyberattacks face mounting compliance costs and higher risks if they do not keep up with new requirements in all markets where they operate.

CyberTrak is designed to help GCs, CIOs, CISOs, risk officers and legal, technology, IT and procurement departments of multinational companies make better, faster risk management decisions and reduce the costs associated with keeping up with these changing regulatory requirements.
CyberTrak content will be regularly updated three times per year by a global group of more than 50 carefully selected contributors in key jurisdictions (many of them contributors to Data Protection Laws of the World), along with interim updates when major changes occur.

Understanding cybersecurity mandates on a global scale is critical to any multinational company that collects and retains customer data, trade secrets, and other confidential data or operates in a critical infrastructure sector, such as energy, financial services, healthcare and defense/government contractors.

Company-wide CyberTrak access is offered on an annual subscription basis. To register for a free trial or to learn more about CyberTrak, please visit www.BlueEdgeLab.com.

Blue Edge Lab, LLC is a wholly owned subsidiary of DLA Piper LLP (US). Blue Edge Lab is not a law firm and does not provide legal services.

**GDPR SITE**

We are proud to present a dedicated site offering DLA Piper’s insight into the General Data Protection Regulation, the once-in-a-generation change in EU data protection laws.

**DATA PROTECTION BLOG**

If you find this Handbook useful, you may also be interested in DLA Piper’s Data Protection, Privacy and Security group’s Privacy Matters Blog, a blog featuring regular data protection, privacy and security legal updates to help you remain aware of the most important legal and regulatory developments.

We have over 130 experienced privacy and security lawyers across the globe who are close to the regulations in each of their respective jurisdictions and who regularly post summary articles on their local issues.

To access the blog, please visit http://blogs.dlapiper.com/privacymatters/.

To ensure you receive an automatic email when a new article is posted, please enter your details in the ‘subscribe’ section found on the blog’s righthand sidebar.

**DISCLAIMER**

This handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements. Furthermore, enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.
DATA PROTECTION AND PRIVACY GROUP KEY CONTACTS

Americas

Jim Halpert
Partner & Chair of US Data Protection and Privacy Group
T +1 202 799 4441
jim.halpert@dlapiper.com

Jennifer Kashatus
Partner, Data Protection, Privacy and Security
T +1 202 799 4448
jennifer.kashatus@dlapiper.com

Europe, Middle East and Africa

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

Prof. Patrick Van Eecke
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +32 2 500 1630
patrick.van.eecke@dlapiper.com

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

Diego Ramos
Partner
T +34 9 1790 1658
diego.ramos@dlapiper.com

Richard van Schaik
Partner & Co-Chair of EMEA Data Protection and Privacy Group
T +31 20 541 9828
richard.vanschaik@dlapiper.com

Asia Pacific

Peter Jones
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group
T +61 2928 68356
peter.jones@dlapiper.com

Scott Thiel
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group
T +852 2103 0519
scott.thiel@dlapiper.com

EDITORS

Kate Lucente
Associate and Co-Editor, Data Protection Laws of

James Clark
Associate and Co-Editor, Data Protection Laws of the
ANGOLA

LAW

Data Protection Law (Law no. 22/11 of 17 June), Electronic Communications and Information Society Services Law (Law no. 23/11, of 20 June 2011) and Protection of Information Systems and Networks Law (Law no. 7/17, of 16 February).

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 deemed to be an individual that may be directly or indirectly identified, notably, by reference to her/his identification number or to the combination of specific elements of her/his physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

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

- philosophical or politic 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

Agência de Proteção de Dados (APD). Although the Data Protection Law provides for the creation of the APD and in October 2016 it has been approved the Organic Statute of APD by Presidential Decree 214/2016 (which is in force), such authority has not yet been created.

REGISTRATION

In general terms, depending on the type of personal data and on the purposes of the processing either:

- prior notification to APD, or
- prior authorisation from the APD,
is required. Please note that in the case of authorisation, compliance with specific legal conditions are mandatory.

The APD may exempt certain processing from the notification requirement. In general terms, notification and authorisation requests should include the following information:

- 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 the conditions for a data subject to execute further rights of access, rectification, deletion, opposition and updating
- any predicted transfers of personal data to third countries
- a general description (which will allow the APD to assess the suitability of the measures adopted to ensure the processing security).

DATA PROTECTION OFFICERS

There is no obligation to appoint data protection officers.

COLLECTION & PROCESSING

In general terms, personal data collection and processing of personal data is subject to express and prior consent from the data subject and prior notification to the APD. However, data subject consent is not required in certain circumstances provided by law.

With respect to sensitive data processing, collection and processing is only allowed where there is a legal provision allowing such processing and prior authorization from the APD is obtained (please note that the authorization may only be granted in specific cases provided by law). If the sensitive personal data processing results from a legal provision, the same shall be notified to APD.

In any case data processing must fulfill the following general principles: transparency, legality, good faith, proportionality, truthfulness, and respect to private life as well as to the 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:

- 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 which do not ensure an adequate level of protection are subject to prior authorization from the APD which will only be granted in case specific requirements are fulfilled. In case of transfers between the companies of 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 however, 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**

The data controller must implement appropriate technical and organizational measures and to adopt adequate security levels in order to protect personal data against 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.

Having regard to the state of the art and the cost of their implementation, 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. Specific security measures shall be adopted regarding certain type of personal data and purposes (notably, sensitive data, call recording and video surveillance).

Also, according to Protection of Information Systems and Networks Law the service providers, operators and companies offering information society services must: (i) guarantee the security of any device or set of devices used on the storage, processing, recovery or transmission of computer data on execution of a computer programme 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 computer emergency.

**BREACH NOTIFICATION**

There is no mandatory breach notification 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 Comunicações, (INACOM) of any breach of security committed with intent or recklessly that leads to destruction, loss, partial or total modification or non-authorized access to personal data transmitted, stored, retained or by 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 is not yet created, the level of enforcement is not significant at this stage.
Electronic Communications

INACOM regulates, inspects and verifies compliance with the Electronic Communications and Information Society Services Law, and applies the penalties related to violations of it. Although, unlike the APD, the INACOM exists, the level of enforcement is still not significant yet.

ELECTRONIC MARKETING

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

The processing of personal data for this purpose may be conducted without data subject consent in specific circumstances, notably:

- when the advertising is addressed to the data subject as representative, employee of a corporate person and
- when the advertising communications are sent to an individual with whom the supplier of a product or a service has already concluded transactions provided the opportunity to refuse was expressly provided to the customer at the time of the transaction and this does not involve an additional cost. In this case, the data subject has the right to oppose to his personal data processing for advertising/direct marketing purposes.

ONLINE PRIVACY

The Electronic Communications and Information Society Services Law establishes the right for all Citizens to enjoy protection against abuse or violations of their rights through the Internet or by 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 protection and safeguarding to their consumer rights and as users of networks or electronic communications services.

In view of the above it is in general not allowed to store 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/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 storing of specific information and the access to such information is only allowed on the condition that the subscriber/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 communication operators may also store traffic data only to the extent required and 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 data and localization data exclusively for the purpose of:

- investigation
- detection or
- prosecution of criminal offences on Information and Communication Technologies (ICT).

**Location data**

The processing of Location Data 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 the processing and the possibility of disclosure to third parties for the provision of value added services.

Electronic communication operators must ensure the possibility to withdraw consent at any time, or temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication. This shall be provided by using simple means, which are free of charge to the user. The processing should be limited to those employees in charge of electronic communications services accessible to the public.

The Location Data may be kept for criminal investigation or evidence purposes.

**KEY CONTACTS**

**VCA – Law Firm**

www.vca-angola.com

- **Orlanda Vuite**  
  Associate  
  ADCA Advogados Angola  
  T +244 926 61 25 25  
  o.vuite@adca-angola.com

- **Carmina Cardoso**  
  Of Counsel  
  T +244 926 61 25 25  
  c.cardoso@vca-angola.com

**DATA PRIVACY TOOL**

You may also be interested in our [Data Privacy Scorebox](http://www.dlapiperdataprotection.com) to assess your organisation’s level of data protection maturity.
ARGENTINA

LAW

Section 43 of the Federal Constitution grants citizens expeditious judicial action to gain access to information about them contained in public and private databases and to demand its amendment, updating, confidentiality, or suppression if it is incorrect.

Personal Data Protection Law Number 25,326 (the ‘PDPL’), enacted in October 2000, provides much broader protection of personal data closely following Spain’s data protection law. On 30 June 2003, the European Commission recognised that Argentina provides an ‘adequate’ level of protection of personal data, in line with the Data Protection Directive (95/46/EC).

DEFINITIONS

Definition of personal data

Personal information or data means ‘any type of information related to identified or identifiable individuals or legal entities’.

Definition of sensitive personal data

Sensitive information or data means ‘personal information revealing racial or ethnic origin, political views, religious beliefs, philosophical or moral stands, union affiliations or any information referring to health or sexual life’.

NATIONAL DATA PROTECTION AUTHORITY

Argentine Personal Data Protection Agency – in Spanish Dirección Nacional de Protección de Datos Personales (DNPDP)

Sarmiento 1118 – 5th Floor
Autonomous City of Buenos Aires
(C1041AAX) Argentina
T +54 11 4383 8512


The DNPDP has enforcement power.

REGISTRATION

Any public or private database formed for the purpose of providing reports, any private database which is not formed exclusively for personal use, and any database formed for the purpose of transferring personal data must be registered with the DNPDP. The registration must include, at least, the following information:

- name and address of the data collector
characteristics and purpose of the database

nature of the data included in the database

collection and update methods

individuals or entities to which the data may be transferred

methods for linking the recorded information

methods used to ensure data security, including a detail of the people with access to information processing

time during which the data will be stored, and

conditions under which third parties can gain access to data related to them and the procedures performed to correct or update the data.

DATA PROTECTION OFFICERS

There is no requirement in Argentina for organizations to appoint a data protection officer.

However, a ‘Head of Data Security’ (Responsable de Seguridad) must be appointed by data controllers to which ‘medium’ or ‘high’ security requirements apply. Its duties are exclusively related to ensuring compliance with database security measures.

COLLECTION & PROCESSING

In general, data controllers may only collect and process personal data with the data subject’s consent. Consent is not required if:

- the data is collected from a publicly accessible database, in the exercise of government duties, or as a result of a legal obligation
- the database is limited to certain basic information, such as name, ID, tax ID, job, birthdate and address
- the personal data derives from a scientific or professional contractual relationship and is used only in such context, or
- the information is provided by financial institutions, provided that they were required to do so by a court, the Central Bank or a tax authority.

When collecting personal data, the data collector shall expressly and clearly inform data subjects of:

- the purpose for which the data is being collected
- who may receive the data
- the existence of a database, the identity of the data collector and its mailing address
- the consequences of providing the data, of refusing to do so or of providing inaccurate information, and
- the data subject’s access, rectification and suppression rights.

In addition, data contained in databases must be truthful, adequate, pertinent, and not excessive, be used exclusively for the purpose for which it was legally obtained and be deleted on completion of that purpose. Incomplete or partially or totally false data must be immediately amended or suppressed.

No person may be required to disclose sensitive personal data. Sensitive personal data may only be collected and processed in cases of public interest, as determined by law. Anonymised sensitive personal data may be collected for statistical or scientific
purposes, so long as the data subjects are no longer identifiable.

Data related to criminal history or background may only be collected by public authorities.

**TRANSFER**


Personal data may only be transferred out of Argentina in compliance with legitimate interests of the transferring and receiving parties, and generally requires the prior consent of the data subject, which may be later revoked.

Consent to the transfer of personal data is not required when:

- the collection of the data did not require consent
- the transfer is made between government agencies in the exercise of their respective duties
- the data relates to health issues, and is used for emergencies, epidemiologic studies or other public health purposes, provided that the identity of the subject is protected, or
- the data have been de-identified such that they may no longer be linked with the corresponding subjects.

The transferee is subject to the same obligations as the transferor, and both parties are jointly and severally liable for any breach of data protection obligations.

Personal data may not be transferred to other countries or international institutions that do not provide an adequate level of protection, unless in cases of judicial or intelligence international cooperation, where Argentina has signed specific treaties with the relevant countries covering this issue, or in case of bank transfers or health issues (provided that the requirements set out above are complied with).

The adequate level of protection requirement may also be met by the parties including in the relevant agreement, data protection provisions similar to those contained in PDPL.

**SECURITY**

The data collector must take all technical and organisational measures necessary to ensure the security and confidentiality of the personal data, so as to avoid its alteration, loss, or unauthorised access or treatment. Such measures must permit the data collector to detect intentional and unintentional breaches of information, whether the risks arise from human action or the technical means used. It is prohibited to record personal data in databases which do not meet requirements of technical integrity and safety.

The level of security that must be provided varies in relation to the sensitivity of the personal data. Regulations distinguish between three possible levels of data security, based on the nature of the data stored in the database, and provide for minimum security requirements for each category.

**BREACH NOTIFICATION**

There are no requirements in the PDPL to report data security breaches or losses to the DNPDP or to data subjects. Nevertheless, all data incidents must be recorded by the data controller in a ‘Security Incidents Ledger’. The DNPDP is entitled to request access to the Security Incidents Ledger when conducting an inspection. Notification may be necessary to mitigate potential violations in the event that the DNPDP starts an investigation and detects a security failure, which constitutes a violation of the data security obligations included in the PDPL.

**ENFORCEMENT**
The DNPDP is responsible for the enforcement of the data protection regime. Either acting ex officio or upon a complaint from a data subject, the National Ombudsman or consumer associations, the DNPDP is entitled to start an investigation when it suspects that the PDPL has been infringed. Administrative sanctions include warnings, suspension of the right to maintain a database, the imposition of monetary fines, ranging from AR$1,000 to AR$100,000 (approximately US$117 to US$11,700 as of January 2015), or the cancellation of the database.

In addition, data subjects may separately recover damages for violations of their data protection rights. The PDPL also modified the Argentine Criminal Code to include personal data crimes, such as knowingly inserting false information in a database, knowingly providing false information from a database, illegally accessing a restricted database, or revealing information contained in a database that the offender was in charge of keeping confidential. Criminal violations are subject to prison terms ranging from one month up to three years, which may be increased by 50% if any person suffers damage as a result of the crime.

**ELECTRONIC MARKETING**

The PDPL will apply to most digital 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 PDPL). In all cases, the data subjects are entitled to exercise their access, amendment and deletion rights as provided in the PDPL.

In particular, the DNPDP’s Disposition No. 4/2009 sets forth that:

- all promotional messages shall include the language from the PDPL’s Section 27:3 and the third paragraph of Section 27 of Decree No. 1558/01 – which set forth a data subject’s right to request suppression of their personal information from marketing databases
- all marketing emails not previously requested or consented to by the data subject shall include as their subject the single word *Publicidad* (promotional), and
- senders of promotional messages shall ensure that all mechanisms needed to honour the data subject’s requests are in place.

On August 5, 2014, Law No. 26,951 was published in the Official Gazette, creating the Argentine National Do Not Call Registry. The purpose of such registry is to protect telephone service users (‘Users’) from abuses by companies using such means to advertise, offer, sell or give non-requested goods and services (‘Advertising Companies’). Users may opt to be included in the Registry for free. Advertising Companies, which will be regarded as data collectors under the PDPL and subject to their obligations, will not be allowed to call any registered User, and will need to, on a monthly basis, verify any updates of such list. The penalties for breaches and other enforcement regulations will be those provided in the PDPL. The application authority will be the DNPDP. The law must be implemented by a Decree, which should have been issued by November 3, 2014; however, as of January 6, 2014 the Decree has not yet been issued.

**ONLINE PRIVACY**

Argentina has not enacted specific legislation governing online privacy, nor has the PDPL issued regulations on this point.

Particularly with regard to automatic data collection programs, the current interpretation of most scholars is that information collected by ‘cookies’ or similar programs does not qualify as ‘personal data’ because such information corresponds to a device and not to the user him or herself.
KEY CONTACTS

Cordova Francos Gorbea D’Aiello Jofre ABOGADOS
www.cfgd.com.ar/

Sebastián Córdova-Moyano
Founding Partner
T +54 11 4311 3571
scordova@cfgd.com.ar

Felipe Oviedo Roscoe
Senior Associate
T +54 11 4311 3571
foviedo@cfgd.com.ar

DATA PRIVACY TOOL

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

LAW

Data privacy/protection in Australia is currently made up of a mix of Federal and State/Territory legislation. The Federal Privacy Act 1988 (Cth) (Privacy Act) and its Australian Privacy Principles (APPs) apply to private sector entities with an annual turnover of at least A$3 million and all Commonwealth Government and Australian Capital Territory Government agencies.

The Privacy Commissioner has power under the Privacy Act to conduct investigations (including own motion investigations), ensure compliance with the Privacy Act and seek civil penalties for a serious/egregious breach or for repeated breaches of the APPs where remediation has not been implemented.

Australian States and Territories (except for Western Australia and South Australia) each have their own data protection legislation applying to State Government agencies (and private businesses’ interaction with them). These acts are:

- 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).

There are also various other pieces of State and Federal legislation that impact on or relate to data protection. For example, the Telecommunications Act 1997 (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) all impact privacy/data protection for specific types of data or for specific activities.

Further, specific regulators have expressed their expectations as to the behavior and controls which regulated entities would have in place (for example, in the case of financial services institutions, the Australian Prudential and Regulatory Authority and, in the case of corporations generally, the Australian Securities and Investment Commission). Finally, over the course of 2017, State and Federal legislation has been amended to reflect an enhanced focus on the protection of minors online. The Attorney-General of New South Wales indicated in November 2016, that the intention of the NSW Government was to table legislation in 2017 which would provide for personal civil rights of action for certain serious interferences of an individual’s privacy, this legislation is yet to be tabled. While motivated through specific high-profile instances of "revenge porn" and similar, it is entirely possible that the legislation (if enacted) could have a broader reach. Our focus here, however, is on the application of the Privacy Act to private sector entities.
Private sector entities are referred to as ‘organisations’. Under the Privacy Act/the APPs, an organisation can be an:

- individual
- body corporate
- partnership
- other unincorporated association, or
- a trust.

DEFINITIONS

Definition of personal data

Personal Data (which is 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.

Definition of sensitive personal data

Sensitive Personal Data (which is 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, or
- biometric templates.

NATIONAL DATA PROTECTION AUTHORITY

The Privacy Commissioner (“Privacy Commissioner”) operating under and through the Office of the Australian Information Commissioner (“OAIC”) is the national data protection regulator responsible for overseeing compliance with the Privacy Act. Its website is currently http://www.oaic.gov.au/.

REGISTRATION

Australia does not maintain a register of controllers or of processing activities. There is no requirement under the current data protection regime (ie the Privacy Act) for an organisation to notify/report to the Office of the Privacy Commissioner on the processing of personal information.

DATA PROTECTION OFFICERS

There is no requirement for organisations to appoint a data protection officer, but it is good and usual practice under the current law and guidance has been issued by the Privacy Commissioner strongly recommending it.

COLLECTION & PROCESSING

An organisation must not collect personal information unless the information is reasonably necessary for one or more of its business functions or activities.
Under the Privacy Act organisations must also take steps, as are reasonable in the circumstances, to ensure that the personal information that the organisation collects is accurate, up-to-date and correct.

At or before the time personal information is collected, or as soon as practicable afterwards, an organisation must take reasonable steps to make an individual aware of:

- its identity and how to contact it
- why it is collecting (or how it will use the) information about the individual
- to whom 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 organisation’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 organisation will deal with such complaint
- whether the organisation is likely to disclose their personal information to overseas recipients and, if so, the countries in which such recipients are likely to be located.

Organisations usually comply with these notification requirements by including the above information in a privacy policy and requiring individuals to accept the terms of that privacy policy prior to collecting their personal information.

One of the biggest issues in practice in respect of collection and compliance with the Privacy Act for organisations is the failure to appreciate that the obligations with respect to the mandatory notification requirements outlined above also apply to any personal information they collect from/via a third party. That is, a separate and independent obligation to notify the mandatory matters arises on the receipt of personal information from a third party, as though the organization had collected such personal information directly from the individual. In contrast to Europe, Australian privacy law does not distinguish between a ‘data processor’ and a ‘data controller’.

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

- the personal information was collected for the primary purpose of such disclosure or a secondary purpose related to (and, in the case of sensitive information, directly related to) the primary purpose of collection and the individual would reasonably expect the organisation 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 organisation
- 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 authorised by law or on behalf of an enforcement agency.

In the case of use and disclosure for the purpose of direct marketing, organisations are required to also 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 are additional to the specific commercial electronic messaging requirements outlined below under the heading “Electronic Marketing” although apply to all forms of direct marketing not only electronic marketing.

Where 'sensitive information' is processed there are additional protections under the Privacy Act which generally provide that an organisation is not allowed to collect 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 authorised by law or a court/tribunal order
- a ‘permitted general situation’ or ‘permitted health situation’ exists; for example the information is required to establish or defend a legal or equitable claim or he/she is a serious treat to the life or health of the 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 non-profit organisation and the information relates to the activities of the organisation and solely to the members of the organisation (or to individuals who have regular contact with the organisation relating to its activities).

An organisation must, on request by an individual, give that individual access to the personal information (and the ability to correct inaccurate, out of date or irrelevant information) that is held about the individual unless particular circumstances apply which allow the organisation to limit the extent to which access is given (and to which correction is performed). These include emergency situations, specified business imperatives and law enforcement or other public interests.

Organisations must also provide individuals with the option of not identifying themselves, or of using a pseudonym, when dealing with that organisation unless it is impractical to do so or the organisation is required (or authorised) 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 organisation 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:

- the organisation 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 it is a step towards ensuring compliance with the ‘reasonable steps’ requirement)
- the individual consents to the transfer. However, under the Privacy Act the organisation must, prior to receiving consent, expressly inform the individual that if he or she consents to the overseas disclosure of the information the organisation will not be required to take reasonable steps to ensure the overseas recipient does not breach the APPs
- a ‘permitted general situation’ applies, or
- the disclosure is required or authorised by law or a court/tribunal order.

**SECURITY**

An organisation must have appropriate security measures in place (ie 'take reasonable steps') to protect any personal information it retains from misuse and loss and from unauthorised access, modification or disclosure. The Privacy Commissioner has issued a 32 page detailed guidance document 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 organisation, and how and by which
government agency it is regulated, as noted above specific requirements or expectations may also exist and with which
organisations should be familiar. An organisation 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**

There is currently no obligation to report breaches to affected individuals or to the OAIC, however, from 22 February 2018
entities with existing obligations to comply with the APPs under the Privacy Act must comply with mandatory reporting
requirements under the mandatory data breach notification regime.

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

- Personal information;
- Credit reporting information;
- Credit eligibility information; or
- Tax file numbers.

In summary, the regime requires organisations to notify the OAIC and affected individuals of "eligible data breaches" (in
accordance with the required contents of a notice). 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:

1. both of the following conditions are satisfied:
   1. there is unauthorised access to, or unauthorised disclosure of, the information; and
   2. a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any
      of the individuals to which the information relates; or

2. the information is lost in circumstances where:
   1. unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and
   2. assuming that unauthorised access or unauthorised access disclosure were to occur, a reasonable person would
      conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to which
      the information relates.

Whilst "serious" harm is not defined in the legislation, the OAIC has released guidance on how serious harm may be interpreted
and assessed by organisations.

The regime also imposes obligations on organisations to assess whether an eligible data breach has occurred where the
organisation 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. Importantly, the OAIC has released guidance indicating that
such assessments must be undertaken by organisations within 30 days of any suspected data breach.

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
Privacy Commission.

**ENFORCEMENT**

The Privacy 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 Privacy Commissioner prefers mediated outcomes between the complainant and the relevant organisation.
Importantly, where the Privacy 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 Privacy Commissioner may also investigate any 'interferences with the privacy of an individual' (ie any breaches of the APPs)
on its own initiative (ie where no complaint has been made) and the same remedies as below are available.
After investigating a complaint, the Privacy Commissioner may dismiss the complaint or find the complaint substantiated and make declarations that the organisation rectify its conduct or that the organisation redress any loss or damage suffered by the complainant (which can include non-pecuniary loss such as awards for stress and/or humiliation). Furthermore, fines of up to A$360,000 for an individual and A$1.8 million for corporations may be requested by the Privacy Commissioner and imposed by the Courts for serious or repeated interferences with the privacy of individuals.

**ELECTRONIC MARKETING**

The sending of electronic marketing (which is referred to as ‘commercial electronic messages’ in Australia) is regulated under SPAM Act 2003 (Cth) (‘SPAM Act’) and enforced by the Australian Communications and Media Authority.

Under the SPAM Act a commercial electronic message 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 contain a functional unsubscribe facility to enable the recipient to opt-out from receiving future electronic marketing.

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 A$1.7 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 and State and Territory privacy laws relating to online / e-privacy, the collection of location and traffic data, or the use of cookies (or any similar technologies). If the cookies or other similar technologies collect personal information of a user the organisation 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 Privacy Commissioner has released detailed guidance on this.

---

**KEY CONTACTS**

**Peter Jones**  
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group  
T +61292868356  
peter.jones@dlapiper.com

**DATA PRIVACY TOOL**

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

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.

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 25 May 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, an ordinance was also passed regulating the exemptions from the obligation to conduct a data privacy impact assessment, the DPIA Exemptions Ordinance (DSFA-AV).

**Territorial Scope**

As concerns the territorial scope of application, the relevant provisions of the (old) DSG 2000 have not been amended, and apply under the DSG as well. Thereunder, the DSG applies to processing of personal data in Austria, as well as processing of personal data in another EU Member State, if such processing occurs for the purpose of an Austrian-based main establishment or a branch office of a data controller. If, however, data are processed in Austria by a data controller organized under civil law which is based in another EU Member State, and the processing does not occur for the purposes of a branch office of such controller in Austria, the DSG stipulates that the laws of the state where the controller is based apply.

**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 DSG does not include any additional definitions or derogations as compared to the GDPR. However, Section 1 DSG, which provides a general basic (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 basic (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 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 Austrian Data Protection Authority (Österreichische Datenschutzbehörde) can be contacted at the following address:

Österreichische Datenschutzbehörde
Wickenburggasse 8
1080 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 (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 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. 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.

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). Furthermore, 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

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 pseudonymised; 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
- 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 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.

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

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 unauthorised 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, 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).

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 shall be 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 (e.g. 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 legal entities is subject to the discretion of the Data Protection Authority, i.e. the Authority may decide to impose fines against the legal entity or the responsible natural person, as appropriate. If the fine is imposed against the legal 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 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, a change which is currently forecast for Spring 2019. 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 does not specifically address (electronic) marketing, while the use of personal data for marketing purposes clearly falls within the remit of the Act. It is arguable that the processing of personal data within the scope of the business is permissible for marketing purposes. However, it is argued that the consent of the data subjects is required.

Electronic marketing is also regulated by the Austrian Telecommunications Act (Telekommunikationsgesetz 2003, '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 or to more than 50 recipients. 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 he or she does 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 2003, TKG), Section 107, 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 or to more than 50 recipients. 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 anonymised 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 anonymised.

**Location Data**

Location Data may only be processed for value added 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 check-box 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.

Traffic Data

Traffic Data held by communications services providers (‘CSPs’) 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 for the purpose of invoicing the services. In such a case, if the invoice has been paid and no appeal has been lodged with the CSP the traffic data must be erased or anonymised within three months.

Location Data

Location Data may only be processed for value added 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, including cookies. The user shall be informed of the storage or processing of his/her data and shall explicitly consent to such storage or processing. Consent can for example be obtained via a pop up or click through agreement. However, consent provided by way of browser settings, or a pre-selected check-box etc. is not sufficient in this respect.

If it is necessary to store data for a short time period for technical reasons, such data must be deleted immediately thereafter.

KEY CONTACTS

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

Stefan Panic
Associate
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 organisation's level of data protection maturity.
There is currently no standalone data protection law in Bahrain. A draft is being reviewed before Parliament but has not yet been officially finalised nor published.

Notwithstanding the above, provisions relating to data protection are generally captured in a number of laws in Bahrain and these suggest that consent from data subjects is required to process and transfer their personal data:

- Constitution of Bahrain 2002 (the ‘Constitution’) protects citizens’ rights to privacy as it contains provisions on confidentiality relating to postal, telegraphic, telephonic and electronic communications
- Amiri Decree No. 15 of 1976 with respect to the Penal Code (the ‘Penal Code’) protects individuals’ right to privacy as it contains provisions on the sanctions against those who disclose information without the consent of the concerned person
- Legislative Decree No. 9 of 1984 with respect to Central Population Register (the ‘Central Population Register Law’) prohibits divulging demographic information and imposes sanctions against those who disclose information without the consent from the concerned person
- Legislative Decree No. 28 of 2002 with respect to Electronic Transactions (the ‘Electronic Transactions Law’) contains provisions protecting the confidentiality of electronic records
- Legislative Decree No. 48 of 2002 with respect to the Telecommunications Law (the ‘Telecommunications Law’) prohibits divulging of any confidential information
- Decree No. 64 of 2006 with respect to the Central Bank of Bahrain and Financial Institutions Law (the ‘CBB Law’) contains provisions relating to confidential information and disclosing such information
- Resolution No. 8 of 2009 with respect to Licensees to implement Lawful Access (the ‘Lawful Access Regulation’) contains provisions protecting the subscriber’s right to privacy in the telecommunications services domain
- Law No. 35 of 2012 with respect to Consumer Protection (the ‘Consumer Protection Law’) protects consumer’s privacy, to maintain personal information and not to exploit it for other purposes
- Law No. 36 of 2012 with respect to Labour Law in the Private Sector (the ‘Labour Law’) covers generally right to privacy of employee’s data
DATA PROTECTION LAWS OF THE WORLD

• Decree No. 16 of 2014 with respect to the Protection of Information and National Documents (the ‘Protection of Information and National Documents Law’) covers the importance of information relating to national security

• The Resolution No. 3 of 2015 with respect to Bulk Messaging (the ‘Bulk Messaging Regulation’) protects recipients from unsolicited and solicited messages

• Law No. 60 of 2014 with respect to Information Technology Crimes (the ‘Information Technology Crimes Law’) mentions the penalties of unlawful taping, capturing or intercepting, by technical means, any non-public transmission of information devices data to, from or within an information technology system

• The Central Bank of Bahrain Rulebook (the ‘CBB Rulebook’) contains provisions relating to customer confidentiality during outsourced services and activities.

DEFINITIONS

Definition of personal data

There is no single definition of personal data under Bahrain laws as each law defines personal data differently. The definition of personal data is captured in the following laws:

The Labour Law defines employees’ personal data as:

• The employee’s name, age, ID number, marital status, house address, and nationality
• Job or occupation and qualification and experiences
• Date of employment, current wage, and all modifications to this wage
• Leave taken and sanctions imposed
• The date of termination of service and the reasons thereof
• Minutes of the investigations conducted with the employee, and
• Supervisors’ reports on the level of the employee’s performance in accordance with regulations enforce at the place of work together with any other papers related to the employee’s service

The Central Population Register Law defines demographic information relating to personal data as:

• Name
• House address
• Place and data of birth
• Gender
• Religion
• Marital status
• Parents’ or spouse’s ID number
• Educational qualification, and
• Occupation.

The CBB Law defines personal information as:

• Name
• House address
• Email address, and
• Phone number

Furthermore, the CBB Law defines confidential information as any information relating to private affairs of any licensee’s customers.

Definition of sensitive personal data
There is no specific definition of sensitive personal data.

**NATIONAL DATA PROTECTION AUTHORITY**

There is no authority which is specifically responsible for data protection. However, the Information and e-Government Authority holds demographic and censors information, facilitates communications between all government entities, and controls these communications.

**REGISTRATION**

None.

**DATA PROTECTION OFFICERS**

There is no requirement in Bahrain for organisations to appoint data protection officers.

**COLLECTION & PROCESSING**

Generally consent is obtained from the individuals when collecting and processing their personal data, in order to avoid any breach of privacy and confidentiality provisions mentioned under Bahrain laws. In certain circumstances, the relevant government authority may waive the requirement for an individual’s consent.

Subject to the Information and e-Government Authority’s approval, the Central Population Register Law gives the right for any governmental or non-governmental bodies to obtain demographic information for its interests or for purposes of fulfilling the requirements of its activities.

**TRANSFER**

The Electronic Transactions Law states that, as long as consent is obtained from the user or subject, and provided such information does not give rise to civil or criminal liability, a network intermediary has the right to transmit, send, receive, or store an electronic record or provide other services with respect to that electronic record. Except in respect of public bodies, the necessary consent may be implicitly given through a positive action.

The Consumer Protection Guidelines states that licensed operators should obtain a subscribers’ express permission before publishing the subscribers’ information or providing it to another licensed operator.

For entities regulated by the CBB, the CBB Rulebook contains provisions on outsourcing activities in the Operational Risk Management section whereby the licensees must ensure that the outsourcing agreements comply with all applicable legal requirements regarding customer confidentiality.

**SECURITY**

The data controller must implement adequate security measures in order to ensure national security and to protect the user’s or subject’s personal data from misuse, modification, or unauthorised access or disclosure.

**BREACH NOTIFICATION**

For entities regulated by the CBB, the CBB Rulebook obliges entities to notify the CBB when there is a breach in data protection.

For entities regulated by the Electronic Transactions Law, in the event of a data breach, help may be sought from named officers of the Ministry of Industry, Commerce and Tourism in order to gain more protection.

**Mandatory breach notification**

There is no mandatory notification required in the event of a data breach.
ENFORCEMENT

The law is enforced when the affected party submits a claim to the competent court in Bahrain. However, there is no formal reporting of court decisions in Bahrain and courts do not rely on a formal system of precedence. This can lead to an increased level of unpredictability in litigious matters.

ELECTRONIC MARKETING

Electronic marketing in Bahrain is subject to the Consumer Protection Guidelines, the Lawful Access Regulation and the Bulk Messaging Regulation established by the Telecommunications Regulatory Authority.

According to the Consumer Protection Guidelines, licensed operators are expected to protect consumers from unwanted, offensive, unsolicited or illegal electronic solicited messages, including live voice solicitations, artificial pre-recorded voice advertisements, electronic mail, electronic wireless messages (e.g. short text messages and multimedia messages) and facsimile messages.

According to the Lawful Access Regulation, a licensee may access the subscriber’s information for marketing purposes or to provide value added services to its subscribers only after obtaining consent from the subscriber.

The Bulk Messaging Regulation regulates solicited and unsolicited messaging. Opt-out principles are adopted whereby text messages are only sent to recipients who have expressly consented to the receipt of the message. Texts may only be sent between 9 am to 8 pm. Licensed operators will take appropriate measures to reduce the number of unsolicited bulk messages which are sent over their telecommunications networks by non-contracted sources.

ONLINE PRIVACY

None.

KEY CONTACTS

Mohamed Toorani
Senior Legal Consultant
T +973 1755 0896
mohamed.toorani@dlapiper.com

Noor Buhusayen
Legal Consultant
T +973 1755 0893
noor.buhusayen@dlapiper.com

Lulwa Alzain
Paralegal
T +973 1755 0891
lulwa.alzain@dlapiper.com

DATA PRIVACY TOOL

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

LAW

The main legal acts regulating personal data protection in Belarus are the Law on Information, Informatisation and Information Protection of 10 November 2008 No. 455 Z (the "Information Protection Law") and the Law on Population Register of 21 July 2008 No. 418 Z (the "Population Register Law").

The acts implemented within the framework of the Eurasian Economic Union should also be taken into consideration, eg the Protocol on Informational Communication Technologies and Informational Interaction within the Eurasian Economic Union, Annex 3 to the Treaty on the Eurasian Economic Union of 29 May 2014.

In 2017, the concept of a new Law on Personal Data was introduced and approved by the President of Belarus. It is expected that a draft Law on Personal Data will be submitted to the parliament by April 2019.

DEFINITIONS

Definition of personal data

According to the Information Protection Law personal data consist of 'basic' and 'additional' personal data of an individual which are subject to the admission to the population registry, as well as other data which allow the identification of such an individual. The basic personal data are defined by the Population Register Law as a closed list of the data including:

- name;
- surname;
- birth date;
- citizenship; and
- address details.

The additional personal data are also defined by the Population Register Law as a closed list of the data, including e.g. data on:

- a spouse;
- children;
- relatives;
- tax obligation; and
- education etc.

Belarus law does not define the notion of "other data which allow the identification of an individual".

Definition of sensitive personal data

There is currently no concept of sensitive personal data under Belarus law.
NATIONAL DATA PROTECTION AUTHORITY

There are two main authorities occupied primarily with overseeing data protection: Operational and Analytical Centre under the President of the Republic of Belarus (the "Centre") and the Ministry of Communications and Informatisation of the Republic of Belarus (the "Ministry").

REGISTRATION

Belarus law does not require the registration of information systems (e.g. databases) that contain personal data or to register as a processor of personal data for private owned information systems. For state information systems Belarus law requires registration with the Ministry regardless whether any personal data are processed in it. Such registration can be carried out for private owned information systems voluntarily. According to the Information Protection Law state information systems are information systems created and/or acquired at the expense of state or local budgets, state off-budget funds, or by means of state legal entities.

DATA PROTECTION OFFICERS

State bodies and legal entities which are carrying out personal data processing shall establish special departments or select employees who are responsible for information protection. If technical methods of information protection are used, e.g. encryption, such state bodies and legal entities must establish a special department for technical information protection.

COLLECTION & PROCESSING

Collection and processing of personal data are subject to the following mandatory conditions:

- to be carried out only with a written consent of the individual to which the personal data belong;
- to be carried out in information systems equipped with information protection systems using technical and cryptographic means of protection certified in accordance with Belarus law; and
- to be carried out having implemented certain legal, organisational and technical measures for personal data protection.

The legal measures may include concluding agreements with an individual whose personal data are collected and processed. Such agreements should stipulate the terms of personal data usage, as well as parties responsibility for breach of such terms.

The organisational measures may include establishing a special entrance regime to the premises where the collection and processing are carried out, and designate a list of employees who can have an access to such premises and data.

The technical measures may include using cryptography and other possible measures of control over information protection to be carried out by state bodies and legal entities on the condition that a special department or employees are selected to oversee information protection in such state bodies and legal entities.

TRANSFER

According to the Information Protection Law, transfer of personal data shall be carried out with written consent of the individual to whom the personal data transferred belongs. There are no specific requirements established for transfer of personal data from Belarus to abroad.

In practice, the employers receiving the personal data of their employees carry out possible measures (legal, organisational, technical etc.) to prevent illegal distribution of personal data and comply with Information Protection Law requirements.

SECURITY

Legal entities and/or individuals using personal data shall carry out in accordance with Belarus law appropriate legal, organisational, technical measures of information protection in order to protect personal data from illegal distribution.

BREACH NOTIFICATION
There are no requirements under Belarus law to report personal data protection breaches either to the state authorities, or the individuals whose personal data are concerned.

**Mandatory breach notification**

There are no mandatory requirements under Belarus law to report personal data protection breaches either to the state authorities, or the individuals whose personal data are concerned.

**ENFORCEMENT**

Enforcement of the Law on Information Protection is primarily carried out by the Ministry and the Centre. Currently Belarus law does not provide for any liability for the breach of the regulation on personal data protection. Belarus law does provide for administrative liability in the form of a fine with (or without) a confiscation of the information protection means used, if applying information protection systems and/or using technical and cryptographic means of protection that are not certified in accordance with Belarus law. The administrative fine amounts up to 20 basic units (approx. EUR 221 as of 11 January 2017) for individuals and up to 200 basic units (EUR 2,211 as of 11 January 2017) for legal entities.

**ELECTRONIC MARKETING**

Electronic marketing is subject to the rules established by the Law on Advertising of 10 May 2007 No. 225 Z (the "Advertising Law") and the Law on Mass Media of 17 June 2008 No. 427 Z (the "Mass Media Law").

According to the Advertising Law names, pen names, images or expressions of Belarusian citizens cannot be used in advertisements without their consent. Distribution of advertisements by means of telecommunication networks (e.g. telephone, telex, facsimile, mobile telephone communications, email) can be carried out only with the consent of the subscriber or the addressee. The advertisement distributor is obliged to immediately stop the distribution of advertising to a subscriber or an addressee who made such a demand.

Individuals and entities whose rights have been violated as a result of the manufacture and distribution of advertisement are entitled to refer to the court with the corresponding claims.

According to the Law on Mass Media, the distribution of information messages and/or material prepared with the use of audio, video recording, motion picture photography and photography containing the image of an individual in the mass media without his consent is allowed only when taking measures against possible identification of this individual by third parties, as well as on condition that the constitutional freedoms and rights are not violated and such distribution is carried out in the public interest. These requirements are not applicable when the distribution is required by the court or enforcement agencies.

**ONLINE PRIVACY**

Belarus law does not specifically regulate online privacy. However, the general requirements applicable to personal data protection apply.
KEY CONTACTS

Sorainen
www.sorainen.com/

Kaupo Lepasepp
Partner
T +372 6 400 900
kaupo.lepasepp@sorainen.com

Mihkel Miidla
Senior Associate, Head of Technology & Data Protection
T +372 6 400 959
mihkel.miidla@sorainen.com

DATA PRIVACY TOOL

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

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 GDPR has been integrated in Belgium through a few new laws. The 'Data Protection Act' of 30 July 2018 provides for the implementation of the GDPR’s 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 Law of 3 December 2017 ('DPA Act')2. Adaptions to sectoral laws relying on the previous Data Protection Act will likely follow.

---

1. See the law.
2. See 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 Data Protection Act builds on the definitions contained in the GDPR and further clarifies some notions, such as the notion of 'government'. 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 Act also clarifies certain concepts such as 'processing in the substantial public interest', the 'processing for journalistic purposes' and introduces new concepts such as 'a joint database'.

I. Art. 5 Data Protection Act.
II. Article 8 para. 1 Data Protection Act.
III. Art. 24 para. 1 Data Protection Act.
IV. 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 (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 Data Protection Act appoints three more regulatory authorities (COC\(^1\), Committee I\(^2\) and Committee P\(^3\)) with varying data protection related competences next to the general Data Protection Authority.

2. Art. 72 para. 2 °7 Data Protection Act.

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. In the public sector the Data Protection Act subjects the controller of processing activities in the context of police services to an obligation to publish a protocol detailing the transfer to a government body or private body based on public interest and compliance with legal obligations.

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 requests the appointment of a DPO depending on the impact of the processing activity namely the high risk it may entail according to article 35 of the GDPR when (i) a private law body processes personal data on behalf of the government or the government 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 government bodies regulated by the Data Protection Act are also required to appoint a DPO. 3

---

1. Art. 21 Data Protection Act.
3. The Center for Missing and Sexually Exploited Children (Child Focus) Art. 8 para. 3 Data Protection Act; Governments for prevention, examination, detection and prosecution of criminal facts or the execution of penalties including the protection against and prevention of hazards for public safety implementing Directive 2016/680 Art. 63 e.v. Data Protection Act; Information and security services bodies Art. 91 Data Protection Act; Bodies for security authorisations Art. 124 Data Protection Act; The coordination department on threat analysis 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. 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
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](http://www.dlapiperdataprotection.com)), 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 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. 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.
The Data Protection Act adds only specificities to the general processing requirements. The age for consent of children in the context of the information society services 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, which is to be kept at the disposal of the DPA, and ensure that these people are bound by a legal, statutory or contractual obligation of confidentiality.\(^2\) The Act provides a list of who or when one can process criminal data by requiring an access management list and confidentiality duties, as described here above.\(^3\)

**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\(^4\) or when personal data is disclosed to these bodies.\(^5\) The special regimes addressed in the Act also enumerate the somewhat more limited data subject rights (rectification and verification), whether or not based on previous legislation.\(^6\)

The Act clarifies that data subject rights, including the right to information in judicial proceedings/decisions, will be accommodated in accordance with the Judicial Code and the Code on Criminal proceedings.\(^7\)

---

1. Art. 7 Data Protection Act.
2. Art. 9 Data Protection Act.
3. Art. 10 Data Protection Act.
5. Art. 12 Data Protection Act.
7. 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
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. Notification requirements regarding transfers were previously embedded in Protocol accords and Royal Decrees which execute the legislation and it is currently unclear if those are being reconsidered. 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

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 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 Act sets out the different anonymization or pseudonymisation requirements.¹ Security measures are also detailed for each special regime but resemble the GDPR.²
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 security measures. 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).

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 Act can be enforced by the data subject or by the Data Protection Authority (DPA)\(^1\). Under the Data Protection Act, a body, organisation or non-profit organisation can 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\(^2\)

The claim for an injunction of the processing activity should be brought before the Court of First Instance\(^3\) except when the personal data is processed in criminal investigations, but there is no single court territorially competent. The DPA can impose administrative fines under article 83 of the GDPR varying from 10,000 EUR to 4% of the global annual turnover\(^4\), but the government and their appointees are exempted\(^5\). A supervisory authority can exercise corrective measures but only over certain governmental bodies enumerated in the article.\(^6\)

Depending on the infringement and the infringer, the controller, processor, competent government body or the appointee can be subjected to criminal sanctions between 800 EUR – 160,000 EUR and a publication of the judgement.\(^7\)
The DPA consists of 6 different Committees. The **inspection committee** of the DPA enjoys the power 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. 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. They can also request further information.

The **dispute committee** will 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 but can also impose periodic penalty payments or administrative fines.

### Specific Regulations 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. The Act exempts the controller not only from respecting data subjects’ rights but also obligations of the controller (eg notification in case of breaches, transfer requirements, etc) and the investigative powers of the DPA.

The 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, contractual and security requirements, or compliance with a code of conduct.

The Act does not include other derogations relating to employment.

---

1. Art. 211 par.3 Data Protection Act.
2. Art. 220 par. 2 Data Protection Act.
5. Art. 221 par. 2 Data Protection Act.
6. Art. 221 par. 1 Data Protection Act.
10. Art. 76 DPA Act.
11. Art. 95 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, a change which is currently forecast for Spring 2019. 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 to most electronic marketing activities, as there is likely to be processing and use of personal data involved (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 provides individuals with the right to object to the processing of their personal data (i.e. a right to ‘opt out’) for direct marketing purposes.

Additionally, 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 or the Data Protection Authority Act include provisions on electronic marketing or online privacy.

**ONLINE PRIVACY**

**Cookies**

Article 5 (3) of the E-Privacy Directive has been implemented into Belgian Law by means of an amendment to article 129 of the Belgian Electronic Communication Act.

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.

In February 2015 the DPA issued a recommendation on the use of cookies with useful guidance relating to the information obligation, the consent requirement and the exemptions.

**Location data**

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.

The processing of location data must in addition also comply with the general rules stipulated by the Data Protection Act.

**Traffic data**

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 location 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

Neither the Data protection Act or the Data Protection Authority Act include provisions on electronic marketing or online privacy.

**KEY CONTACTS**

Prof. Patrick Van Eecke  
Partner & Co-Chair of EMEA Data Protection and Privacy Group  
T +32 2 500 1630  
patrick.van.eecke@dlapiper.com
DATA PRIVACY TOOL

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

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 are not yet in force but are expected to come into force in late 2018.

Apart from PIPA, Bermuda law recognizes a duty of confidentiality in certain circumstances under the common law.

DEFINITIONS

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

PIPA makes provision for the office of a Privacy Commissioner. Certain sections of PIPA dealing the Privacy Commissioner were brought into force on 2 December 2016 but a Privacy Commissioner has yet to be appointed.

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.

**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.

**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

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation’s level of data protection maturity.
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 entered into force on 4 July 2006 and its current version (after amendments made in 2011) is in force from 3 October 2011.

DEFINITIONS

Definition of personal data

The DP Law defines personal data as any information relating to an identified or identifiable natural person. The 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/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

- 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.

NATIONAL DATA PROTECTION AUTHORITY

The Personal Data Protection Agency (‘DPA’) is the national data protection authority in BiH. The DPA is seated in

Vilsonovo šetalište 10
Sarajevo
www.azlp.gov.ba

REGISTRATION

Each data controller (defined as a person or legal entity which processes personal data) has to provide the DPA with specific information on the database containing personal data (‘Database’) established and maintained by the controller. The DPA keeps
publicly available register of data controllers and Databases.

The Database’s registration includes two phases:

1. the first phase represents notification of intention to establish the Database to the DPA
2. the second phase includes reporting 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
  - its name, and
  - address of its registered seat, and
- 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 etc.

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.

**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.

**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 needed, written consent has to contain 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 legitimate. These conditions are considered the basic principles of personal data protection and are applicable to each case of personal data processing. For example, 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 which guarantee legitimate reasons for personal data processing.

The DP Law provides for the 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 fulfilment 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’).
TRANSFER

Under the transfer rules set out in the DP Law, processed personal data may be transferred to countries where 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’), since it is considered that countries – members of the Convention ensure adequate level of personal data protection.

Personal data transfer to countries which do not provide for 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 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.

SECURITY

The DP Law prescribes that both data controllers and, within the scope of their competencies, the processors are required:

- to take care of data security and to undertake all technical and organizational measures
- to 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
- to adopt 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.

Moreover, 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.

Manner of personal data keeping and personal data protection in automatic processing is also closely regulated by the Rules.

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’ users.

When it comes to the notification duty towards the users, the Regulation B obliges the Operator to inform the users adequately (eg in user agreement, in its terms and conditions or in the appropriate technical way) about the possibility of privacy or telecommunication facilities violations.

**ENFORCEMENT**

Enforcement of the DP Law is done by the DPA. 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/entity processing personal data acted contrary to the data processing rules, it may request from the controller to 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 misdemeanour proceeding against the respective data controller before the competent court, depending on the gravity of the particular misconduct and the data controller’s behaviour with respect to the same. The offences and sanctions are explicitly prescribed by the DP Law, which includes monetary fines for a controller in the amount between approximately EUR 2,550 and EUR 51,100, as well as for the controller’s authorized representative in the amount between approx. EUR 100 and EUR 7,700.

Breach of personal data protection regulations represents a criminal offence 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 Brko 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 Brko Distrikt) or up to one (1) year (Criminal Code of the Republic of 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 the Regulation B, the Operator is not allowed to use personal data of the users for the purposes of its business or other promotions, unless it obtained explicit consent from the users to whom such data relates.

**ONLINE PRIVACY**

The general data protection rules, as introduced by the DP Law, are relevant for on-line privacy as well, as there are no specific regulations that explicitly govern on-line 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/

Mirna Milanovi Lalic
Senior Associate
T +387 33 261 535
mirna.lalic@karanovic-nikolic.com

Lana Deljkic
Senior Associate
T +387 33 261 535
lana.deljkic@karanovic-nikolic.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation’s level of data protection maturity.
BRITISH VIRGIN ISLANDS

LAW

There is currently no formal legislation regulating data protection in the British Virgin Islands (BVI) however, the BVI Government has pledged the promulgation of suitable data protection legislation, based on internationally recognised standards, to be enacted in the near future.

English Common law is persuasive (although not binding) in the BVI and accordingly, a BVI Court will recognise and subscribe to the Common law duties of confidentiality and privacy. In essence, a person’s details will need to be kept confidential provided an appropriate and satisfactory exception applies. Moreover, the duty of confidentiality has been statutorily codified in various aspects of BVI legislation, in particular the Banks and Trust Companies Act, 1990 (as amended) which regulates all banking and trust/ fiduciary related activities in the BVI.

In terms of specific exceptions, limitations on the duty of confidentiality and privacy would arise in terms of appropriate anti money laundering legislation (primarily regulated by the BVI Proceeds of Criminal Conduct Act, 1997 and the Anti Money Laundering Regulations, 2008).

DEFINITIONS

Definition of personal data

No specific definition at present. Data Protection Bill to be promulgated in the near future which will contain definitions as appropriate.

Definition of sensitive personal data

No specific definition at present. Data Protection Bill to be promulgated in the near future which will contain definitions as appropriate.

NATIONAL DATA PROTECTION AUTHORITY

No specific data protection authority at present pending promulgation of data protection legislation in the near future. The Courts of the BVI would be guided by English Common law duties of confidentiality and privacy. Moreover, the Financial Services Commission (the ‘Commission’) regulates the fiduciary and trust business sectors, pursuant to the Banks and Trust Companies Act, 1990 (as amended).

REGISTRATION

No specific mechanisms of registration pending the promulgation of data protection legislation in the near future.

DATA PROTECTION OFFICERS
There is presently no requirement for the appointment of data protection officers in the BVI.

**COLLECTION & PROCESSING**

Entities, which manage and maintain personal information data will be subject to the Common law duty of confidentiality. From a fiduciary/trust perspective, licensees are under a general obligation to maintain the privacy and confidentiality of a client’s personal information unless specific permission is granted for its release or dissemination to third parties. This obligation may however be limited pursuant to the requirements of appropriate anti money laundering legislation/ regulations.

From a corporate perspective, the Registrar of Corporate Affairs (the ‘Registrar’) is able to release only limited information regarding the particulars of any registered company including the name, type of company, the date of registration/incorporation, the address of its registered office and the status of the company. Accordingly, details of shareholders and directors are not available for public inspection (unless specifically authorised and filed by the company itself). Except where assistance to law enforcement agencies to combat illicit activity is mandated or authorised, disclosure of information by government officials, professional agents, attorneys and accountants and their employees is prohibited.

**TRANSFER**

Transfer of data to third parties would be subject to the Common law duty of confidentiality (which may include a statutory duty (where the Common law duty of confidentiality has been codified) depending on the nature of data being transferred). A transferor would need to ensure that appropriate measures have been taken in order to obtain the necessary consents/ approvals prior to such data being disseminated.

On 1 September 2014 the Computer Misuse and Cybercrime Act, 2014 came into force which regulates and penalises the unauthorised transfer and dissemination of information stored on a computer.

The Commission is under a general obligation of confidentiality but has the power to disclose in certain circumstances, including disclosure to foreign regulators in approved jurisdictions of information necessary to enable the regulator to exercise similar functions to those exercised by the Commission. However, before doing so, the foreign regulator is required to undertake that the information will not be transmitted to any other person without the prior written consent of the commission.

**SECURITY**

There are no formal statutory security measures currently in place (pending the promulgation of appropriate data protection legislation in the near future), however the holder would be subject to a general obligation to ensure the technical and organisational safeguarding of such confidential information and personal data.

**BREACH NOTIFICATION**

There is no current mechanism or requirement in place to report data security breaches in the British Virgin Islands.

**ENFORCEMENT**

Presently, the Commission and the BVI Courts will be tasked with the enforcement of data protection and confidentiality related matters (insofar as applicable pending promulgation of appropriate data protection legalisation).

**ELECTRONIC MARKETING**

No formal electronic communications regulations or legislation currently in place however, the Telecommunications Act (No 10 of 2006) regulates the telecommunications industry in the British Virgin Islands and provides sanctions protecting the confidentially and disclosure of personal information.

**ONLINE PRIVACY**

No such legislation at present in the British Virgin Islands.
KEY CONTACTS

Carey Olsen
www.careyolsen.com

Alan Hughes
Senior Associate
T +1 284 494 4030
alan.hughes@careyolsen.com

DATA PRIVACY TOOL

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

Last modified 24 May 2018

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 Act was last amended by the State Gazette, Issue No. 103 of 28 December 2017, which came into force on 1 January 2018.

In the view of the entry into force of Regulation (EU) 2016/679 (General Data Protection Regulation - 'GDPR'), on 30.04.2018 a draft law amending and supplementing the Personal Data Protection Act ('Draft Law') was introduced for public discussion. The objectives of the Draft law are to ensure the effective implementation of the GDPR and the fulfillment of the obligations of the Republic of Bulgaria as an EU Member State with respect to transposing into national legislation Directive (EU) 2016/680 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 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 Draft Law 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 Draft Law.

The Draft law designates the Commission for Personal Data Protection as the sole supervisor responsible for protecting the fundamental rights and freedoms of individuals with regard to the processing and free movement of personal data within the European Union. The Draft law 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 the Draft 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 personal data

The Draft law repeals the definition of personal data as described in the current Personal Data Protection Act and explicitly refers to the definition of personal data under art. 4 of the GDPR (§1 of the Supplementary provisions of the Draft law).

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 Draft law repeals the definition of sensitive data under the current Personal Data Protection Act and implies that the definition under the GDPR would apply 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 (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 Bulgarian data protection authority (DPA) is the Personal Data Protection Commission (In Bulgarian: Комисия, 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 (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 Draft Law repeals the current requirement for registration before the local DPA. Pursuant the Draft law the DPA shall maintain the following public registers:

- register of data protection officers;
- register of the accredited certifying bodies under art. 14;
- register of codes of conduct.

The DPA shall also support an internal register of established breaches of the GDPR and the Personal Data Protection Act, as well as a register of the measures taken in accordance with art. 58, para 2 of the GDPR, which however shall not be made public.
The rules for maintaining the registers, their content and access thereto shall be regulated in Rules of Procedure to be adopted by the DPA.

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.

Apart from the cases under art. Art. 37, para (1) of the GDPR, the Draft law requires a Data Protection Officer ("DPO") to be appointed when processing personal data of more than 10 000 individuals.

Pursuant to the Draft law, data controllers shall be further obliged to communicate the names and contact details of the DPO, as well as any subsequent replacements, before the Commission, and will also have to publish their contact details. The form and content of the notification and the procedure before the Commission shall be regulated in the Rules of Procedure of the Commission and its administration to be adopted by the DPA.

In addition, the Draft law specifies that the DPO may perform his / her duties under employment or civil-service relationship, incl. when performing a job under another position at the controller. In addition, the Draft law explicitly prohibits data controller and data processors from performing the functions 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. 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 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. 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.

The Bulgarian Draft law does not repeat the core provisions of the GDPR relating to collection and processing of personal data in its body, but directly refers to Art. 6, para (1) (legal grounds for processing) and Art. 5 (principles for data processing) GDPR (art. 25a of the Draft law). In case the data subject provides his / her personal data to a data controller or a data processor in breach of these provisions, 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.

The Draft law also introduces additional rules relating to specific data processing situations:

- Conditions applicable to child’s consent in relation to information society services - The Draft law introduces lower age of 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 Draft law 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 - The Draft Law addresses a topic which was largely discussed by data subjects and data controllers – the personal identification number possessed by each Bulgarian citizen. Should the Draft Law be adopted, public access to personal identification number / personal identification number of a foreigner (‘PIN/PINF’) shall be granted only if required by law. The law should define the terms and conditions of granting such access, in order to prevent that the PIN/PINF is made publicly available, where ‘public availability’ means the disclosure of personal data or otherwise providing access to them to an unlimited number of persons without taking measures to ensure accountability. 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 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 assessment should be made based on a number of criteria, such as:

  - the type of personal data; the impact the public disclosure of the personal data would have on the privacy of the data subject and his/her reputation; the circumstances under which the personal data have become known to the data controller; the character and nature of the statement by which the freedom of expression and information has been exercised; the importance of the disclosure of personal data for clarifying a matter of public interest; whether the data subject is a person who holds a position under Art. 2, para. 1 of the Public Disclosure of Financial Interests of Officials Holding High State and Other Positions Act or is a person who, due to the nature of his / her activity or role in public life, has a lesser degree of protection of his / her privacy or whose actions have an impact on society; whether the data subject has contributed to the disclosure of his / her personal data and / or information on his or her personal and family life; the purpose, content, form and consequences of the statement by which the freedom of expression and information has been exercised; the compliance of the statement by which the freedom of expression and information has been exercised, with the fundamental citizens rights; other circumstances relevant to the particular case.

The data controller’s decision should not disproportionately restrict the freedom of expression and information.
• Processing in the context of employment - The Draft law regulates explicitly certain matters related to personal data processing in the context of employment relationship. The Draft Law provides that employers may copy employee’s identification document, driving license or residence document only if required by law. The 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 Draft law 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 three years. In cases where for the purposes of the recruitment the employer has 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 position occupied, the non-hired data subject may request to receive back the submitted documents within 30 days of the final closure of the recruitment procedure, whereas the employer should return the documents in the same manner they were submitted. Finally, the Draft law provides that employers may process personal data of an employee which have not been requested or which are not required by statutory law, if the data subject has given his/her explicit consent therefor and if such processing is not prohibited by statutory law.

• Personal data processing by way of large-scale surveillance of publicly accessible areas - Under the Draft law data controllers and data processors shall adopt special rules for the processing of personal data through systematic large-scale surveillance of publicly accessible areas, including via video surveillance. The Draft law 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 surveilled, 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 DPA.

Processing of personal data of deceased persons

The Draft law 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, incl. a copy thereof, to his/her heirs or other persons with legal interest.

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:

- 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 Draft law 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.

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:

- 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.

The Draft law does not derogate form the provisions of the GDPR regarding security of personal data and does not introduce any additional rules or requirements in this respect. After the entry into force of the GDPR the current DPA’s
**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 Draft law 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.

**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 Draft law designates the DPA as the overall supervision and control regarding compliance with the GDPR in Bulgaria. The Draft law defines the competences of the Commission by referring to art. 57 and 58 of the GDPR. Apart from performing the powers under the GDPR, the DPA shall be entitled to:

1. analyze and carry out overall supervision and ensure compliance with the GDPR, the Draft law and the legislative acts in the area of personal data protection;
2. issue secondary legislation in the area of personal data protection;
3. 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;
4. participate in international cooperation between data protection authorities and international organizations on personal data protection issues;
5. participate in the negotiation and conclusion of bilateral or multilateral agreements on matters within its competence;
6. organize, coordinate and conduct training in the field of personal data protection;
7. issue administrative acts related to its authority in the cases provided for by law;
8. adopt criteria for the accreditation of certification bodies;
9. issue guidelines, recommendations and best practices in cases where such are not issued by the European Data Protection Supervisor.
10. bring proceedings before the court for breach of the GDPR;
11. issue mandatory instructions, give instructions and recommendations regarding the protection of personal data;
12. impose coercive administrative measures.

The Commission is also entitled to further clarify in its internal Rules of Procedure its tasks, procedures and rules for work of its administration, as well as rules for the proceedings before the Commission. With respect to the administrative sanctions, the Draft law sets the amount of the fines depending on which provision of the GDPR or of the Draft law has been violated. It also introduces minimum amounts of fines to be imposed:

- for violations described in Art. 83, para. (5) and para. (6) of the GDPR and for breaches of Art. 45, para. 1, Art. 49, para. 1, Art. 52, Art. 54-56, Art. 80, para. 1, item 1, letter “a”, item 2, letter “b” and letter “c” of Chapter Eight [of the Draft law] the data controller / data processor shall be subject to a fine or a pecuniary sanction at the amount of 10,000 up to the equivalent of EUR 20,000,000;
- for violations under Art. 83 (4) of the GDPR, Art. 59, Art. 62, Art. 64-69 of Chapter Eight [of the Draft law] the data controller / data processor shall be subject to fine or a pecuniary sanction at the amount of BGN 5,000 up to the equivalent of BGN 10,000,000;
- for other violations under the Draft law the data controller / data processor shall be subject to a fine or a pecuniary sanction of 1000 up to 5000 BGN;

For other violations of the GDPR the data controller / data processor may be subject to mandatory instructions or a fine / pecuniary sanction at the amount of BGN 2,000 up to BGN 200,000 under the terms and conditions set forth in Art. 84 and Art. 87 [of the Draft law].

The DPA 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.

Data controllers are liable for any damage caused to an individual as a result of unlawful processing or by breaching the technical requirements of data protection. The data controller is also liable for any damage caused by a data processor acting on behalf of the data controller.

In case of a violation of his/her rights under the GDPR and the Draft law, every data subject is entitled to refer the matter to the DPA within one year of becoming aware of the breach, but no later than five years from the breach taking place. 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 no 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 2 April 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, a change which is currently forecast for Spring 2019. 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 Draft law does not introduce any rules relating specifically to e-marketing. As the Draft law explicitly refers to the legal grounds for processing of personal data under the GDPR, thus including also the area of e-marketing, the explicit consent of the data subject is likely to be the only applicable ground for the purposes of e-marketing. The absence of a special legal framework concerning exclusively data protection in e-marketing makes the option regime the only possible legitimate method of pursuing e-marketing.

In addition, although the Draft law repeals the provision of the current 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 Ecommerce Act explicitly requires, when it comes to direct marketing to natural persons, the option mechanic to be mandatorily applied. Moreover, 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 latest 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, the relevant text in the Electronic Commerce Act states that users should be provided with clear and comprehensive information about the purposes of data processing in accordance with the Personal Data Protection Act and they must be given the opportunity to refuse to the storage or access to such information. In practice the DPA interprets the law as an opt-in regime.

**KEY CONTACTS**

*Wolf Theiss*
www.wolftpiss.com/

Anna Rizova
Partner
Wolf Theiss
T +359 2 8613703
anna.rizova@wolftpiss.com
DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation's level of data protection maturity.
DATA PROTECTION LAWS OF THE WORLD

CANADA

Last modified 24 January 2017

LAW

In Canada there are 28 federal, provincial and territorial privacy statutes (excluding statutory torts, privacy requirements under other legislation, federal anti-spam legislation, identity theft/ criminal code etc.) that govern the protection of personal information in the private, public and health sectors. Although each statute varies in scope, substantive requirements, and 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 ('PIPA Alberta')
- Personal Information Protection Act ('PIPA BC'),
- Personal Information Protection and Identity Theft Prevention Act ('PIPITPA') (not yet in force), and
- An Act Respecting the Protection of Personal Information in the Private Sector ('Quebec Privacy Act'), (collectively, 'Canadian Privacy Statutes').

PIPEDA applies:

1. to consumer and employee personal information practices of organisations that are deemed to be a ‘federal work, undertaking or business’ (eg banks, telecommunications companies, airlines, railways, and other interprovincial undertakings)

2. to organisations 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 Privacy Act have been deemed ‘substantially similar’), and

3. to inter provincial and international collection, use and disclosure of personal information.

PIPA BC, PIPA Alberta and the Quebec Privacy Act apply to both consumer and employee personal information practices of organisations within BC, Alberta and Quebec, respectively, that are not otherwise governed by PIPEDA.

DEFINITIONS

Definition of personal data

‘Personal information’ includes any information about an identifiable individual.

Definition of sensitive personal data

Not specifically defined.
NATIONAL DATA PROTECTION AUTHORITY

1. Office of the Privacy Commissioner of Canada (‘PIPEDA’)
2. Office of the Information and Privacy Commissioner of Alberta (‘PIPA Alberta’)
3. Office of the Information and Privacy Commissioner for British Columbia (‘PIPA BC’), and
4. Commission d’accès à l’information du Québec (‘Quebec Privacy Act’)

REGISTRATION

There is no registration requirement under Canadian Privacy Statutes.

DATA PROTECTION OFFICERS

PIPEDA, PIPA Alberta, PIPA BC and PIPITPA expressly require organisations to appoint an individual responsible for compliance with the obligations under the respective statutes.

COLLECTION & PROCESSING

Canadian Privacy Statutes set out the overriding obligation that organisations 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 be opt in or opt out. Organisations 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, organisations 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 organisations make information about their personal information practices readily available.

All Canadian Privacy Statutes contain obligations on organisations to ensure personal information in its 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 organisation.

Each of the Canadian Privacy Statutes also provides individuals with:

1. a right of access to personal information held by an organisation, subject to limited exceptions, and
2. a right to correct inaccuracies in/update their personal information records.

Finally, organisations must have policies and practices in place that give effect to the requirements of the legislation and organisations must ensure that their employees are made aware of and trained with respect to such policies.

TRANSFER

When an organisation transfers personal information to a third party service provider (ie who acts on behalf of the transferring organisation), the transferring organisation remains accountable for the protection of that personal information and ensuring compliance with the applicable legislation. In particular, the transferring organisation is responsible for ensuring 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.
With respect to the use of foreign service providers, PIPA Alberta specifically requires a transferring organisation 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 authorised to collect, use or disclose personal information for or on behalf of the organisation.

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 organisation’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 organisation 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 organisation.

In addition, under the Quebec Privacy Act, an organization must take reasonable steps to ensure that personal information transferred to service providers outside Quebec will not be used for other purposes and will not be communicated to third parties without consent (except under certain exceptions prescribed in the Act). The Quebec Privacy Act also specifically provides that the organization must refuse to transfer personal information outside Quebec where it does not believe that the information will receive such protection.

SECURITY

Each of the Canadian Privacy Statutes contains safeguarding provisions designed to protect personal information. In essence, these provisions require organisations to take reasonable technical, physical and administrative measures to protect personal information against loss or theft, unauthorised 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, PIPA Alberta and PIPITPA are the only Canadian Privacy Statute with breach notification requirements. However, proposed amendments to PIPEDA would require notice of material breaches to be made to the Office of the Privacy Commissioner of Canada (‘OPC’) and, in certain circumstances, to the individuals affected.

In Alberta, an organisation having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorised access to or disclosure of the 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 unauthorised access or disclosure
- the date or time period during which the loss or unauthorised access or disclosure occurred
- a description of the personal information involved in the loss or unauthorised access or disclosure
- an assessment of the risk of harm to individuals as a result of the loss or unauthorised 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 unauthorised access or disclosure
- a description of any steps the organisation has taken to reduce the risk of harm to individuals
• a description of any steps the organisation has taken to notify individuals of the loss or unauthorised access or disclosure, and

• the name and contact information for a person who can answer, on behalf of the organisation, the Commissioner’s questions about the loss of unauthorised access or disclosure.

Where an organisation suffers a loss of or unauthorised access to or disclosure of personal information as to which the organisation is required to provide notice to the Commissioner, the Commissioner may require the organisation 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 unauthorised access or disclosure

• the date on which or time period during which the loss or unauthorised access or disclosure occurred

• a description of the personal information involved in the loss or unauthorised access or disclosure

• a description of any steps the organisation has taken to reduce the risk of harm, and

• contact information for a person who can answer, on behalf of the organisation, questions about the loss or unauthorised access or disclosure.

In Manitoba, an organisation must, as soon as reasonably practicable, notify an individual if personal information about the individual that is in its custody or under its control is stolen, lost or accessed in an unauthorized manner. This requirement to notify an individual does not apply where:

• the organisation is instructed to refrain from doing so by a law enforcement agency that is investigating the theft, loss or unauthorized accessing of the personal information, or

• the organisation is satisfied that it is not reasonably possible for the personal information to be used unlawfully.

The exact form of the notice that must be provided to individuals has not yet been prescribed.

On 8 April 2014, proposed amendments to PIPEDA were introduced that, if passed, would require that organisations report to the OPC ‘any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual’. The proposed amendments also require organisations to notify an affected individual ‘if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual’. The proposed amendments are not yet in force.

ENFORCEMENT

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 organisation 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 organisation 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. Organisations 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 $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 Privacy Act, an order 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.

A failure to comply with the Quebec Privacy Act’s requirements in respect of the collection, storage, communication or use of personal information is liable to a fine of up to $10,000 and, for a subsequent offence, to a fine up to $20,000. Any one who hampers an inquiry or inspection by communicating false or inaccurate information or otherwise is liable to a fine of up to $10,000 and, for a subsequent offence, to a fine of up to $20,000.

Under the PIPITPA, it is an offence to (a) willfully collect, use, or disclose personal information in contravention of the Act, (b) willfully attempt to gain or gain access to personal information in contravention of the Act, and (c) dispose of or alter, falsify, conceal or destroy personal information or any record relating to personal information, or direct another person to do so, with an intent to evade a request for access to information or the record. A person who commits an offence is liable on summary conviction, in the case of a person other than an individual, to a fine of not more than $100,000.

**ELECTRONIC MARKETING**

Electronic marketing is governed by both Canadian Privacy Statutes (as discussed above), as well as Canada’s Anti-Spam Legislation (‘CASL’).

Under CASL it is prohibited to send, or cause or permit 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 the Act and 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 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 (ie 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 $1 million per violation for individuals and $10 million for corporations (subject to a due diligence defence). CASL also sets forth a private right of action permitting individuals to bring a civil action for alleged violations of CASL ($200 for each contravention up to a maximum of $1 million each day for a violation of the provisions addressing unsolicited electronic messages).

**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, and
- the collection, use and disclosure of personal information on social networking sites. 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 behavioural 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 behavioural advertising.

In ‘Privacy and Online Behavioural Advertising’ (the ‘OBA Guidelines’), the OPC stated that it may be permissible to utilize opt-out consent in the context of online behavioural advertising if the following conditions are met:

- individuals are made aware of the purposes for the online behavioural 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 behavioural 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 behavioural advertising must not be a condition of service and, as a best practice, should not be used on websites directed at children.

With respect to location data, such information, whether tied to a static location or a mobile device, is considered to be personal information by Canadian privacy regulatory authorities. 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? and
- Are there less privacy-intrusive alternatives to achieve the same objective?
KEY CONTACTS

Tamara Hunter
Associate Counsel
T +1 604.643.2952
tamara.hunter@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation’s level of data protection maturity.
CAPE VERDE

LAW


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.

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**

There is no obligation to appoint a data protection officer.

**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 the following two requirements are met:

- the express and unambiguous consent of the data subject has been obtained
- the data protection authority has been notified.

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 is no formal requirement for breach notification, nor is there formal requirement for mandatory breach notification.
ENFORCEMENT

Enforcement of the Data Protection Law is done by the data protection authority. 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

CV Lexis
www.mirandalawfirm.com/

Antonio Ferreira
Partner
T +238 261 13 44
praia@cvlexis.com

DATA PRIVACY TOOL

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

LAW

There is no legislative framework currently in force in the Cayman Islands that specifically addresses issues of data protection. The Data Protection Law, 2017 (the Law) was passed by the Legislative Assembly of the Cayman Islands on March 27, 2017, but this and any regulations issued under it are not expected to come into force until some time in January 2019. The precise date the Law will come into force will be set by Cabinet Order.

Notwithstanding the lack of data protection legislation in force, the Cayman Islands does recognise a duty of confidentiality in certain circumstances, under both the common law and, implicitly, the provisions of the Confidential information Disclosure Law 2016 of the Cayman Islands (the CIDL). The CIDL functions primarily to enumerate a non-exhaustive list of instances in which disclosure may lawfully be made. The CIDL also repeals the previous Confidential Relationships Preservation Law (as revised) of the Cayman Islands, which regulated disclosures of confidential information by professional persons and provided, among other things, for criminal sanctions for certain breaches of confidentiality on an extra-territorial basis.

DEFINITIONS

Definition of personal data

There is no definition of "personal data" contained in any legislation currently in force.

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

There is no definition of "sensitive personal data" contained in any legislation currently in force.

NATIONAL DATA PROTECTION AUTHORITY

There is currently no "Data Protection Authority" in the Cayman Islands. However, when the Law comes into force the Information Commissioner, for the purposes of the data protection regime, will be the person appointed under section 35 of the Freedom of Information Law (as revised), who at present primarily addresses freedom of information issues in the Cayman Islands.

REGISTRATION

Not applicable for this jurisdiction (see National Data Protection Authority section).

DATA PROTECTION OFFICERS
There is currently no requirement to appoint a data protection officer.

**COLLECTION & PROCESSING**

There are no statutory provisions currently in force that specifically address the collection and processing of personal information.

At common law, however, it is generally 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.

In the context of confidential information received by a professional person in the context of a professional relationship with a principal, the CRPL provides that a person is guilty of a criminal offence where he or she "clandestinely, or without the consent of the principal, makes use of" any confidential information for his or her benefit or the benefit of another.

**TRANSFER**

Absent a breach of an obligation of confidentiality at common law, there is no specific statutory regulation of the transfer of information from or within the Cayman Islands. For entities regulated by the Cayman Islands Monetary Authority (CIMA), the latter has issued guidance in relation to the outsourcing of core functions by regulated entities to third party service providers that impacts on the transfer, storage and processing of customer confidential information.

**SECURITY**

There are no statutory provisions in force mandating that specific measures be taken to protect against or prevent disclosure or other unlawful use of confidential information. However, a person who misuses or divulges confidential information (deliberately or otherwise) may be liable at common law or under the CRPL.

**BREACH NOTIFICATION**

There are no general requirements to notify any authority or any other person of a breach of confidentiality.

**ENFORCEMENT**

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 courts of the Cayman Islands.

**ELECTRONIC MARKETING**

There are no specific restrictions addressing the use of confidential information in electronic marketing beyond those generally applicable to the use of confidential information.

**ONLINE PRIVACY**

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

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

Elaine Gray
Partner
Carey Olsen
T +44 1481 72 72 72
elaine.gray@careyolsen.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation’s level of data protection maturity.
DATA PROTECTION LAWS OF THE WORLD

CHINA

LAW

Currently, there is not a comprehensive data protection law in the People’s Republic of China (‘PRC’). Instead, rules relating to personal data protection are found across various laws and regulations. Generally speaking, provisions found in laws such as the General Principles of Civil Law and the Tort Liability Law may be used to interpret data protection rights as a right of reputation or right of privacy. However, such interpretation is not explicit.

Nevertheless, 2017 was a ground-breaking year for cybersecurity and data privacy for the PRC. The PRC Cybersecurity Law (promulgated and effective from 1 June 2017) adopted by the Standing Committee of the National People’s Congress has become the first national-level law that addresses cybersecurity and data privacy protection.

Further to the Cybersecurity Law, the following form the backbone of general data protection rules currently in the PRC:

- The Decision on Strengthening Online Information Protection (Promulgated and effective on 28 December 2012; the ‘Decision’) adopted by the Standing Committee of the National People’s Congress; and

(collectively referred to as the ‘General Data Protection Law’). The purpose of the Decision 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. The Decision has the same legal effect as a law. While the Guideline is only a technical guide and thus not legally binding, it is considered important because its scope extends to any “processing of personal information through information systems” (not necessarily connected to the Internet), and because of the fact that it covers in detail key issues such as data exports, sensitive data, data subject access and the right to rectification. Given the lack of binding laws and regulations which provide detailed guidance on data processing, the Guideline can be a good reference. Therefore, compliance with the Guideline is recommended as good practice.

In addition to the General Data Protection Law, provisions contained in other laws and regulations may be applicable depending on the industry or type of information at issue (for example, personal information obtained by financial institutions, e-commerce businesses, certain healthcare providers, or telecom or Internet service/content providers is subject to special regulation). For example (this is not an exhaustive list):

- The Criminal Law of the People’s Republic of China prohibits sale or illegal provision of, or illegal access (such as theft) to citizens’ personal information;
- Provisions of the Supreme People’s Court on Several Questions relating to the Applicable Law of Civil Disputes Concerning the Use of Informational Network to Harm Personal Rights and Interests (promulgated on 21 August 2014, and effective on 10 October 2014), which are applicable to Internet users and Internet service providers who use
A significant recent development is the Information Security Techniques - Personal Information Security Specification, which was issued on 29 December 2017 and comes into force on 1 May 2018 (the "PI National Standards"). While the formal text of these standards have not been made available to the public, the draft versions indicate that they set out key data protection concepts and principles which until now remain elusive and have not been properly developed or explained in key laws and regulations, including the Cybersecurity Law. The PI National Standards may not necessarily replace the Guideline issued in 2012 in theory, but they are expected to be the new national standards on personal data protection in China.

Please note that our discussion here only includes the General Data Protection Law and the drafts of the PI National Standards that are available currently (not the final version) as such laws will have the most direct, general and broad application to most if not all types of businesses in the PRC. Applicability of other laws or regulations will invariably depend on the factual context of each case and further independent analysis is recommended, (for example, businesses in the banking, healthcare or securities sectors will be subject to industry-specific data protection regulations; and employee personal data attracts some protections under employment laws).

DEFINITIONS

Definition of personal data

There is no single, pervasive definition of personal data in the PRC, but the definitions in the various laws, regulations and guidance that comprise the data protection framework in the PRC are starting to become more aligned.

Personal data (which is referred to as ‘personal information’ in the Decision) means any electronic information which can enable identification of a citizen’s individual identity and which relates to personal privacy. This definition was further clarified in the Guideline as any data or information in connection with a specific individual, which can be used, separately or in combination with other data, to identify the individual.

Under the Cybersecurity Law, personal information is defined as including all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person’s identity, including, but not limited to, the natural persons’ full name, date of birth, identification numbers, personal biometric information, addresses, telephone numbers and so forth.

The definition has been further expanded to include information reflecting an individual’s activities under the Interpretations on Several Issues Concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens’ Personal Information issued by the Supreme People’s Court and the Supreme People’s Procuratorate of China on 9 May 2017.

Definition of sensitive personal data

The draft PI National Standards make a distinction between sensitive personal information and general personal information. In the draft PI National Standards, sensitive personal information is defined as personal information the leakage, illegal provision or abuse of which may harm personal/property safety and personal reputation or physical/mental health, or result in discrimination towards the data subject. Examples may include personal identification number, individual biometric information, bank account
number, correspondence records and contents, property information, credit information, location tracking, lodging information, health and physiological information and transaction information etc.

The binding laws or regulations including the Decision, the Consumer Protection Law and the Cybersecurity Law do not make such distinction.

**NATIONAL DATA PROTECTION AUTHORITY**

The CAC (Cyberspace Administration of China) is currently considered the data protection authority in the PRC, although there are also sector-specific regulators that may monitor and enforce data protection issues, such as the PBOC or CBRC which regulate banks and financial institutions.

**REGISTRATION**

The PRC does not maintain a register of data administrators, personal data processing activities or databases containing personal information.

**DATA PROTECTION OFFICERS**

There is no legal requirement in the PRC for organizations to appoint a data protection officer.

The draft PI National Standards however require that an institution or personnel be appointed to be responsible for personal data protection. A data protection specialist / division exclusively handling data protection matters is required if i) the primary business of an organization is related to data processing and there are more than 200 employees; or ii) personal data of more than 500,000 individuals are processed, or personal data of more than 500,000 individuals is expected to be processed within 12 months.

**COLLECTION & PROCESSING**

Clear consent is required from the data subject before the personal information can be processed.

Under the Decision, the Consumer Protection Law and the Cybersecurity Law, organisations caught by those rules may collect and use personal information if the following conditions are met:

- abide by the principles of legality, legitimacy and necessity, and may not be excessive;
- explicitly notify the purposes, means and scope of collection, use and disclosure of personal information;
- obtain the data subject's clear consent to the personal information collection, use and disclosure;
- not violate laws, regulations or agreements between the organisation and the data subject when collecting or using the personal information; and
- make publicly available the organisation's rules or policy regarding collection and use of personal information.

Under the draft PI National Standards, a Data Controller should make a privacy policy which is designed to inform data subjects about the ways in which their personal data is collected, processed and disclosed. It must in particular contain 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;
- the list of personal data collected for each business purpose, processing policies including location of storage, retention period, frequency of collection, etc.;
- whether the data requested from the internet user is optional or mandatory (usually identified by means of an asterisk on the website) and the consequences of any failure by the internet user to provide such data;
- 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.);
- the circumstances under which the Data Controller will share, assign personal data to third parties or publicly disclose personal data, the types of personal data involved in the sharing, assignment or disclosure, and the types of third party data recipients, as well as their legal obligations;
The basic data security principles to be followed by the Data Controller, the data security capabilities of the Data Controller, as well as the data protection measures to be adopted by the Data Controller;

the rights of data subjects and mechanisms for them to realize these rights, e.g. methods to access, rectify, delete their personal data, methods to de-register their accounts, withdraw their consent, and to obtain copies of their personal data, methods to restrict automated decision by the data system etc.;

potential risks for providing personal data, as well as possible impacts for not providing the data; and

channels and mechanism for making inquiries and lodging complaints by data subjects, as well as external dispute settlement body and contact information.

The information in the "data protection policy" must be true, accurate and complete. The contents of the "data protection policy" must be clear and easy to understand, follow common language habits, use standard numbers and graphics for illustration etc., and ambiguous language should be avoided. An abstract of the "data protection policy" should be provided at the beginning of the policy, stating the key points of the notified information. The "data protection policy" should be published publicly and easily accessible. When changes occur to the information provided in the data protection policy, data subject should be notified of such changes.

Collection from persons under 14 years old is prohibited unless consent is obtained from their legal guardians.

Data subject rights to access, rectify the data, obtain copies or request deletion of the data, to withdraw consent or de-register accounts etc. are granted under the draft PI National Standards.

The rules do not apply to truly (and irreversibly) anonymised data according to the Cybersecurity Law and the Draft Consumer Protection Regulations.

TRANSFER

The Cybersecurity Law prohibits disclosure or transfer of an individual's personal information to others without the individual's consent. It further includes requirements for personal information of Chinese citizens and "important data" collected by key information infrastructure operators ("KIIOs") to be kept within the borders of the PRC. If there are business needs for the KIIOs to transfer this data outside of the PRC, security assessments must be conducted. The definition of KIIOs remains to be clarified.

Data localisation is an increasing trend in the PRC, with various sector specific regulations prohibiting transfer of personal information outside the borders of the PRC.

In principle, it is not allowed to share or assign the personal data. If it is really necessary to do so, adequate attention to risks should be paid. The following requirements for sharing and assigning of personal data should be complied with, if the sharing and assigning personal data is not because of acquisition, merger or restructuring:

- perform prior assessment on the impact to the security of personal data, and take effective measures to protect the data subjects according to the assessment results;
- inform the data subjects of the purposes of the sharing and assigning of the personal data and the types of data recipient, and obtain prior express consent from the data subjects;
- before any personal sensitive data is shared or assigned, e.g. ID number, property information, health data etc., inform the data subjects of the identity and data security capabilities of the data recipient, and obtain prior express consent from the data subjects (in addition to complying with the requirements listed in the above);
- record accurately and keep the information in relation to the sharing or assigning of the personal data, including the date, scale, purpose and basic information of the data recipient of the sharing or assigning;
- must not share or assign any personal biometric information; and
- assist the data subjects in understanding the storage and use of personal data by the data recipient, including the rights of the data subjects, such as access, correction, deletion and cancellation of accounts.

If you are a third party (Data Processor) who is delegated to process personal data, the following requirements should be complied with:
• the Data Controller should perform an assessment on the delegation in respect of the influence on the security of personal data, and ensure the Data Processor has adequate data security capabilities and has provided adequate level of protection;
• the Data Controller should supervise the Data Processor, e.g. by conducting audits over the Data Processor; and
• accurate record of the delegation history should be kept; and
• the Data Controller should require the Data Processor to comply with certain obligations through a contract.

SECURITY

Organizations 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.

Under the Cybersecurity Law, network operators are required to establish information protection systems. In particular, network operators must implement technical and other necessary measures to ensure the security of personal information and to prevent the collected data from being accidentally disclosed, tampered with or destroyed. Remedial measures must be taken immediately if personal information is being or is likely to be disclosed, tampered with or destroyed. Network operators should also establish systems 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.

China has implemented a tiered system for cybersecurity protection. Information systems are classified into 5 tiers and the security standard goes higher from tier 1 to tier 5. The regulators leave the protection of tier 1 and tier 2 information systems to their respective organizations and they would only intervene in the case of tier 3, 4 and 5 information systems where national security is a concern. Organizations should conduct a self-evaluation and determine the tier it belongs to, based on relevant laws, regulations and guidelines, inter alia, the Information Security Technology - Classification Guide for Classified Protection of Information System. If an organization considers its information system a tier 3 system, it will need to conduct an assessment with a third party assessment agency to verify whether it meets the standards for tier 3 information system, obtain a test report, and conduct a filing with the Public Security Bureau (based on the test report issued by the agency). If it is deemed as a tier 2 information system, an organization is required to make the filing with PSB without having to conduct a security assessment or obtain a report. A tier 2 information system owner is recommended (but not required) to conduct a security assessment with a third party agency every two years.

BREACH NOTIFICATION

The current laws and regulations including (inter alia) the Cybersecurity Law only provide the following general requirements for reporting and notification of personal data breach, without specific or clear guidance on the timeline for reporting and without identifying which government agencies are in charge (clarifications are pending in this regard):

• network operators should adopt technical and other necessary measures to ensure the security of personal data they collected. Where personal data is leaked, lost or distorted (or if there is a potential for such incidents), network operators must promptly take relevant measures to prevent the aggravation of the damages and promptly notify relevant data subjects and report to relevant government agencies in accordance with relevant provisions.

On the other hand, the draft PI National Standards provide detailed guidance on reporting and notification of personal data breaches or security incidents:

Contingency Response and Reporting of Security Incidents:

• A contingency plan for security incidents of personal data should be formulated;
• Organize trainings of contingency response and contingency drills regularly (at least once a year), in order to let relevant internal staff understand their responsibilities, strategies and procedures for contingency response;
• When a data breach/ security incident occurs, the following actions should be taken in terms of the contingency response plan:
  ○ record the content of the incident, including but not limited to: the person who discovers the incident, the date,
place, personal data and number of people involved in the incident, the name of the system in which the incident occurs, impact on other interconnected systems, whether the law enforcement department or other relevant department have been contacted;
- assess the possible impact of the incident, and take necessary measures to control the situation and eliminate potential dangers;
- if applicable, report to relevant government agency in accordance with the "National Network Security Incident Contingency Response Plan", the content of report shall include but not limited to: general information such as the type, number, content and nature of the data subjects involved, potential impact of the incident, measures taken or to be taken, contact details of relevant persons involved with handling the incident; and
- update the contingency response plan in a timely manner pursuant to the changes of relevant laws and regulations as well as the situation of the incident.

**Notification of Security Incidents:**

- Notify data subjects of relevant information of the incident by mail, letter, telephone, push notification or other means in a timely manner. If it is hard to notify each data subject, organizations shall take reasonable and effective measures to publish warning message relevant to the public;
- The content of the notification shall include but not limited to:
  - the content and impact of the security incident;
  - the measures taken or to be taken;
  - suggestions for data subjects regarding how to take initiative to prevent and reduce the risk of security incidents;
  - remedies specifically provided for data subjects; and
  - contact persons and organizations responsible for personal data protection.

**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. The PRC currently lacks a centralised enforcement mechanism for data protection and there is no single data protection authority or any other state agency established to monitor the protection of personal data. CAC which was relatively newly established to regulate cyberspace issues is expected to be the key data protection authority for enforcement actions, although other industry-specific regulators should also be relevant.

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.

Typically, it would be a graded approach - warning and requirement to comply, then possibly fines up to approximately RMB500,000. Affected individuals may also potentially claim for indemnification under the Tort Liability Law. In severe cases, breaches may lead to higher fines being imposed or the revocation of licence. Responsible personnel could be prohibited from engaging in relevant business and their conduct could be recorded in their social credit files. Depending on the severity of the illegal conduct, the responsible person could also be subject to detention or up to seven years of imprisonment, plus a concurrent fine to the organisation if applicable.

The data protection provisions provided by the Criminal Law have been the most widely used provisions to enforce privacy protection in the PRC. Essentially, only the illegal sale or purchase of personal data are subject to enforcement under the Criminal Law.

However, the enforcement environment is evolving rapidly as individuals are increasingly aware of their data protection rights and as data protection obligations expand as laws develop and are added in China. For example, the Cybersecurity Law suggests the possibility of ordering corrections, issuing warnings, confiscation of illegal gains and fines of up to 10 times of illegal gains (or fines of up to RMB1,000,000 where there is no illegal gain) upon discovery of violation in handling personal information. The responsible persons may also be fined between RMB 10,000 to 100,000.
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.

Each electronic message must state the identity of the entity sending the message: name, contact information and offer a simple means of opposing the sending of further marketing messages. Every email of direct marketing must be marked as “(advertisement in Chinese) or “AD” at the beginning of the subject.

The current Chinese law is not clear or specific on the rules of marketing over telephone. Telemarketing (over the phone) or below-the-line marketing (by post) should be allowed in the event that prior consent of the targets is secured expressly (i.e. data subjects have opted-in).

There are specific rules applicable to direct marketing by text messages, i.e., the opt-in should include the following additional information compared to the requirements for other electronic means such as email: (i) frequency of sending the text messages (e.g. once every month, or once every one to three months etc.); and (ii) duration of time for which the recipient will be receiving the text messages, e.g. [x] years.

ONLINE PRIVACY

The Decision indicates that network service providers and other companies should ensure the privacy of personal electronic information. They are not allowed to disclose, falsify, damage, as well as sell or unlawfully provide personal electronic information to anyone else. The Consumer Protection Law and the Cybersecurity Law offer similar protection to consumer/user personal information as well.

The Decision also indicates that network service providers should strengthen management of information provided by users. Also, network service providers should stop the transmission of unlawful information and take necessary measures to remove them and save relevant records, then report to supervisory authorities.

Once citizens find network information that discloses their identity or breaches their legal rights, or are harassed by commercial electronic information, they have the right to require that the network service provider delete related information or take measures to prevent such behaviours.

Data subject rights to correction of their data, as well as a right to request deletion of data in the event of a data breach, are also provided by the Cybersecurity Law, which generally prescribes data protection and data security obligations by network operators.

Under the Decision, network service providers must require users to provide genuine identification ("real name") information when signing agreements to grant them access to the Internet, fixed-line telephone or mobile phone services or to permit users to make information public.

In relation to online privacy for mobile apps the "Provisions on Administration of Information Services of Mobile Internet Application Programs" require app providers to adopt real-name registrations and verify users’ identities based on mobile phone numbers or other information. Providers are prohibited from collecting users’ location data, reading their contacts, starting the recording function or camera or any other irrelevant functions without clear notification and users’ consent. Furthermore, app publishers are required to undertake information content review and management mechanisms including to punish anyone releasing illicit information through warnings, limitation of functions, cessation of updates, or shutting down accounts.

There are currently no specific requirements regarding cookies within existing laws or regulations in the PRC.
KEY CONTACTS

Scott Thiel
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group
T +852 2103 0519
scott.thiel@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation’s level of data protection maturity.
COSTA RICA

LAW

The development of data privacy regulation in Costa Rica is divided among two laws (the "Laws"). The first law is Law No. 7975, Undisclosed Information Law, which makes it a crime to disclose confidential/personal information without authorization. The second law is Law No. 8968, Protection in the Handling of the Personal Data of Individuals, and its by-laws were enacted regulate the activities of companies that administer databases containing personal information. Therefore, its scope is limited.

DEFINITIONS

Definition of personal data

Personal information contained in public or private registries (e.g. medical records) that identifies or could be used to identify a natural person. Personal information can only be disclosed to persons/entities with a 'need to know' such information.

Definition of sensitive personal data

Personal information relating to ideological orientation, creed, sexual preferences. 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, hereinafter "PRODHAB", is the entity charged with enforcing compliance with the applicable regulation.

Pursuant to the abovementioned By-Laws, PRODHAB has to be granted by each data holder, for control purposes, with unrestricted and permanent access to each data base through a “Superuser”. This policy has been a very controversial requirement in Costa Rica.

The Constitutional Court also has 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 in any manner such personal information must register before 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 and manage a database containing personal information if the following rules are respected:

- When accumulating 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, express and valid consent from the owner of the personal information or its 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;
  - accurate; and
  - individuals have access to their personal data and must be entitled to dispute any erroneous or misleading information about them.
- Individuals must have access to their personal data and must be entitled to dispute any erroneous or misleading information about them at any time.
- Companies that manage databases containing personal information and that commercialize 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 before PRODHAB.
  - Report the technical issues related to the security of the database.
  - Protect and respect confidentiality issues
  - Secure the information contained in the databases; and
  - Establishing a proceeding to review requests filed by individuals for the amendment of any error or mistakes in the database.

TRANSFER

Transfer of personal information is authorized by the Laws if the data subject provides prior, express and valid written consent to the company that manages the database. Such transfer cannot violate the principles and rights granted in the Laws.

Transferring of public information (which has general access) does not need authorization from the data subject.

SECURITY

Any company or individual using and/or managing this type of information must take all necessary steps (technical and organisational) to guarantee that the information is kept in a safe environment. 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

There is no mandatory requirement. Nonetheless, if there is a breach the entity that manages the database might be liable.

ENFORCEMENT

PRODHAB recently announced that they will begin to enforce the obligations established under the Laws. Therefore, individuals may file their claims directly to PRODHAB so they may initiate an administrative procedure against database manager.

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, do apply.

**KEY CONTACTS**

**FACIO & CAÑAS**

www.fayca.com/

Carlos J. Oreamuno
Partner
T +(506) 2233 9202
coreamuno@fayca.com

Sergio A. Solera
Partner
ssolera@fayca.com

**DATA PRIVACY TOOL**

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

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 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 Ope uredbe o zaštiti podataka) was enacted in the Croatian Parliament on 27 April 2018 and came into force on 25 May 2018 (the '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
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 (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.

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 (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 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.

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 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](http://www.dlapiperdataprotection.com)), 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 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. 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.

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 - 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.

The Act does not contain any special transfer requirements other than those prescribed by 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 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 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 (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, a change which is currently forecast for Spring 2019. 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 on-line privacy as well. AZOP is in charge of control of all on-line data processing.


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**

**Karanovic & Nikolic**


**Danijel Pribani**

Senior Associate  
T +385 1 5601 330  
danijel.pribanic@karanovic-nikolic.com
DATA PRIVACY TOOL

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

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
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 Bill 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 (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 authority designated under the Bill 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 Bill 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 enforcement of measures restricting the rights referred to under Article 12 and 15 until 22 of the GDPR.
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 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 Bill, 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. 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 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. 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.

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 Bill impact assessment and prior consultation with the Commissioner is 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 and 15 until 22 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, defence, 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 organisation 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 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.

With regards to processing of special categories of personal data, prior to such data being transferred to a third country or an international organisation on the basis of appropriate safeguards provided for under Article 46 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.

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 derogations or additional requirements introduced by the Bill 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 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 Bill limits the obligation of the data controller to notify data subjects for breaches of personal data. The data controller may be exempted from such an obligation for one or more of the purposes listed in Article 23(1) of the GDPR, including inter alia, national security, defence, 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 
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).

According to the Bill, 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, with regards to Article 83 of the GDPR, the Bill provides that the administrative sanction imposed in relation thereto shall not exceed EUR 200,000).

With regards to breaches of, inter alia, Articles 30, 31, 33, 34, 35, 42 and of Chapter V of the GDPR, the Bill provides that any such breach shall constitute a criminal offence which may result in the imposition of imprisonment up to three (3) years and/or monetary fines up to EUR 30,000 (where the breach was due to negligence) or imprisonment up to five (5) years and/or monetary fines up to EUR 50,000 (where the breach was intentional).

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 (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, a change which is currently forecast for Spring 2019. 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 (e.g an e-mail 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 fourteen (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](http://www.dlapiperdataprotection.com) to assess your organisation’s level of data protection maturity.
CZECH REPUBLIC

Last modified 24 May 2018

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 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 law has not been passed in the Czech Republic yet and will likely not be passed soon.

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.

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 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. 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 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.

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, a change which is currently forecast for Spring 2019. 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 keep 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).

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 still using the ‘opt-out’ principle because the user must be informed and explicitly allowed to refuse the cookies storage (no prior consent required). The ‘opt-in’ principle as introduced by the Directive 2009/136/EC has not been implemented into Czech law, although many state authorities, including the Office, publicly declared the opposite. Nevertheless, due to the above-mentioned ambiguity, we cannot exclude the risk that the Office will require the prior consent to be given by visitors of the relevant web-site according to the generally applicable obligation under the Act, if the relevant cookie is able to identify the specific user.

Relevant supervising and enforcing authorities in this area are primarily the Office and to some extent also the Czech Telecommunication Office.

KEY CONTACTS

Jan Rataj
Senior Associate
T T +420 222 817 800
jan.rataj@dlapiper.com

Stanislav Bedná
Senior Associate
T T +420 222 817 310
stanislav.bednar@dlapiper.com

DATA PRIVACY TOOL

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

LAW

By order on the EU Council, the General Data Protection Regulation (EU) 2016/679 (‘Regulation’) entered into force on 25 May 2018. To implement the Regulation, the Danish Parliament enacted the Danish Act on Data Protection (‘Act’) on 17 May 2018, enforceable on 25 May 2018 and replacing the Danish Act on Processing of Personal Data (Act no. 429 of 31/05/2000). Hence, data protection and processing is now in Denmark regulated by the Regulation supplemented by the Act.

The Act does not apply for Greenland and the Faroe Islands.

DEFINITIONS

Definition of personal data

“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.

In Denmark, information relating to deceased persons is considered Personal data as well until 10 years after perishing.

Definition of “processing”

“Processing” is 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.

A “data controller”

Meaning 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.

A Processor

Meaning the natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

(The abovementioned definitions correspond to the definitions as set out in the Regulation.)

NATIONAL DATA PROTECTION AUTHORITY
Datatilsynet (“DPA”)
Borgergade 28, 5
DK 1300 København K

T +45 3319 3200
F +45 3319 3218

REGISTRATION

In Denmark, the following types of processing requires 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;
- transfer of Special Categories of Personal Data, originally processed for scientifically and statistically purposes, if i) such data is to be processed outside the geographical scope of the Regulation, ii) the data constitutes biometric data or iii) if the data is to be published in a well-known paper.
- processing personal data in a register on behalf of a private data controller:
  - solely for the purpose of warning other businesses from engaging business 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

Under the Regulation, organisations 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 designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in the Regulation.

Under the Danish Act, the DPO is subject to a duty of secrecy and are prohibited against transfer and exploiting any personal data processed in their capacity of being DPO.

COLLECTION & PROCESSING

The Regulation differs between 1) Personal data, 2) Special Categories of Personal Data, 3) Data on criminal offences and 4) Social security numbers. See below.

1. Personal data

Data controllers may legally register and process personal data (all data except the Special Categories of Personal Data, Data on criminal offences and Social security numbers) when at least any 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 Regulation; or
- 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; or
- processing is necessary for compliance with a legal obligation to which the controller is subject; or
- processing is necessary in order to protect the vital interests of the data subject or any other natural person; or
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.

Under the Act, it is legal to process data on children with a minimum age of 13. Data on children younger than 13 years old, is only legal if the child’s parents or legal guardians have given their explicit consent.

2. Special Categories of Personal Data

Special Categories of Personal Data (as detailed under “Registration”) may be processed only when at least any 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: or
- 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 and other specific rights such as social security and social protection law; or
- 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; or
- 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; or
- processing relates to personal data which are manifestly made public by the data subject; or
- 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. 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.

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 passed on, unless at least any of the following conditions are met:

- the data subject concerned has given his or her explicit consent in accordance with article 7 in the Regulation; or
- the pass on is performed to attend private or public interests, significantly overriding consideration of non-disclosure and the data subject’s interests in general; or
- the pass on is necessary for the performance of regulatory and public business or for a public authority to decide on a ruling; or
- the pass on is necessary for the performance of either a natural person or a company’s tasks on behalf of public authorities.

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 in the Regulation, 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 passed on without the explicit consent
of the data subject, unless such pass on is performed in the interests of either the public or private data controller or the data subject in question conditioned that these interests significantly exceeds the consideration of non-disclosure.

Both public and private actors may process data relating to criminal convictions and offences if at least one the following conditions are met:

- 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 and other specific rights such as social security and social protection law; or
- 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; or
- 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; or
- processing relates to personal data which are manifestly made public by the data subject; or
- 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. The DPA must approve the processing unless such is carried out by the public organization.

4. Social security numbers

Social security numbers (in Danish and henceforth “CPR-no.”) may be processed by public organisations for the purpose of identification or as reference number.

Private data controllers may process CPR-no. when at least one of the following conditions are met:

- the process is required under statutory law; or
- the data subject concerned has given his or her explicit consent in accordance with article 7 in the Regulation; or
- the processing is carried out for scientifically og statistically purposes (however not for publication which requires a specific consent); or
- the CPR-no. is passed on as part of the company’s natural operations and such pass on is of significant importance to the company to ensure identification of the data subject in question or requested by a public authority; or
- 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 and other specific rights such as social security and social protection law; or
- 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; or
- 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; or
- 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 legal claims or whenever courts are acting in their judicial capacity; or
- processing is necessary for reasons of substantial public interest. The DPA must approve the processing unless such is carried out by a public data controller.

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 legal basis for the process in details;
• the recipients or categories of recipients of the personal data, (if any);
• (where applicable), information of transfer of data or the intention hereof;
• The period for which the data will be stored;
• 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)

Under the Act the above-mentioned obligation does not apply if interests of the public, other privates or the data subject itself exceeds the data subject’s interest in obtaining the information.

TRANSFER

The Danish Act does not regulate transfer of personal data. Thus, the articles hereof in the Regulation 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, and on 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 concludes the standard terms approved by the EU-Commission.

If no judgement 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 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

SECURITY

The Danish Act does not set out provisions on security requirements. Thus, the articles hereof in the Regulation applies, 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 Act.

BREACH NOTIFICATION
The Danish Act does not set out provisions on notification in case of security breach. Thus, the articles hereof in the Regulation applies, under which the data must notify the DPA no later than 72 hours after becoming aware of the security breach.

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**

The DPA, which consists of a Council and a Secretary, is responsible for the supervision of all processing operations covered by the Act.

The DPA can request any information provided necessary for the DPA’s operations including decision-making on whether Act and the Regulation apply or not.

The DPA and its personal can without a court order request access to premises from which processing is 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 hereof, 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 Act, is sanctioned with a fine or prison for up to 6 months.

In general, the Regulation 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 5 years.

**ELECTRONIC MARKETING**

The Regulation applies to electronic marketing activities involving usage of personal data (e.g. an email address which includes the recipient’s name).

Under the Regulation companies cannot pass on 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 Regulation 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) can, however, be passed on 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 passing on 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, e-mail, 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 mentioned, a trader that has received a customer’s electronic contact details in connection with the sale of products may market own 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 an ePrivacy Regulation, a change which was forecasted for spring 2018, however, now postponed until spring 2019. 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 Regulation.

ONLINE PRIVACY

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 25 May 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 25 May 2018 (the “Cookie Order”).

The Cookie Order should be read in the light of Regulation, 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. Finally, the consent must be an informed indication of the user’s wishes.

Normally, consent is obtained through tick-the-box but also the use of a homepage after having received the relevant information concerning cookies can constitute consent. Yet consent by use of a homepage must be used with caution.

In addition to this, the information to the user must fulfil the below mentioned requirements:

- the information must be clear and easy to understand
- the purpose of the use of the cookies must be provided
- the identity of the person or entity which is responsible for the use of the cookies must appear
- the possibility of withdrawal of consent must be easily accessible and be described in the information, and
- this information must be easily accessible for the user at all times.

The ePrivacy Directive is to be replaced by an ePrivacy Regulation which is expected enacted in spring 2019. Hence, the above mentioned rules are expected to change.

From the wording of the latest draft, it is unsurprisingly safe to say that the definition of consent used in the Regulation 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 of 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.
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 organisation’s level of data protection maturity.
EGYPT

LAW

Egypt does not have a law which regulates protection of personal data. However, there are some piecemeal provisions in connection with data protection in different laws and regulations in Egypt. Further, a draft law regulating the freedom of data exchange and data protection was drafted, but it has not yet been approved or published. It is expected to be discussed before the Egyptian parliament.

Constitutional principles concerning individuals’ right to privacy under the Egyptian Constitution as well as general principles on compensation for unlawful acts under the Egyptian Civil Code govern the collection, use and processing of personal data.

In addition, the Egyptian Penal Code no. 58/1937 imposes criminal punishment for unlawful collection of images or recordings for individuals in private places. Some other laws provide for protection and confidentiality on certain data, such as the Egyptian Labour Law no. 12/2003 (confidentiality of the employee’s file information including punishment and assessment) and the Egyptian Banking Law no. 88/2003 (confidentiality of client and account information). Egyptian Civil Status Law no. 143/1994 provides for the confidentiality of citizens’ civil status data. The Executive Regulations of Mortgage Finance Law no. 148/2001 issued by virtue of Cabinet Decree no. 1/2001 as amended by Prime Minister Decree no. 465/2005 has a similar clause which provides for the confidentiality of the data of the clients of mortgage finance companies. The Egyptian Telecommunications Law no. 10/2003 provides for the privacy of telecommunications and imposes penalties which account to imprisonment in some cases on the unauthorized violation of such privacy. Egyptian Penal Code no. 58/1937 and Physicians Code of Ethics provide for the privacy of the patient’s information and prohibition to disclose it without the patient’s prior consent. The violation of such prohibition could be penalized by imprisonment and/or minimal fines.

Article 57 of the Egyptian Constitution promulgated in January 2014 provides for the protection of privacy and secrecy of, inter alia, mails, phone conversations and other methods of communication. The aforementioned shall not be monitored, inspected or confiscated unless by virtue of a prior court order and for a limited period of time as regulated by the law.

The Egyptian Constitution has not defined data protection. However, it refers to the legislative authority to regulate the communication of data in a manner that does not encroach upon the privacy of citizens, their rights and National Security.

DEFINITIONS

Definition of personal data

There is no definition of personal data or private life under Egyptian law or the Constitution. However, Egyptian laws provide examples of the personal data that are protected such as the Labour Law. Article 77 of the Labour Law provides that the employees’ files that must be kept by the employer (as mentioned below) includes the employee’s personal data such as his name, job, professional skills when he joined the workplace, domicile, marital status, salary, starting date of his work, the holiday leave he takes, punishments imposed on him and the reports of his superiors on his work.
Definition of sensitive personal data

There is no definition of sensitive personal data under Egyptian law.

NATIONAL DATA PROTECTION AUTHORITY

There is no national authority responsible for data protection in Egypt.

REGISTRATION

There is no requirement or facility to register data in a specific register.

DATA PROTECTION OFFICERS

There is no requirement in Egypt for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

According to the principles of the Egyptian Civil Code, the collection, use or processing of personal data is prohibited in case it violates the individual right to privacy and provided that such collection, use or processing constitutes a fault pursuant to the Egyptian Civil Code. A fault is defined by the judiciary as an act or omission that violates an obligation imposed by the law or assumed caution and care of the average man.

Only data which is considered pertinent to the data subject’s private life requires the consent of the data subject. The competent courts will determine whether specific data is considered pertinent to the private life of the data subject or not and whether the collection or processing of such data violates an obligation imposed by the law or assumed caution and care of the average man.

Collecting data about the employee is required by law (Article 77 of the Egyptian Labour Law) which provides that each employer must keep a file for each employee which includes their personal data. Only certain persons are authorised by the law to have access to such data.

TRANSFER

The same general principles applicable to data collection and processing mentioned above apply to the transfer of data. The data controller may not transfer data pertinent to the private life of the data subject except after obtaining the consent of the data subject, unless otherwise permitted by the law.

SECURITY

Other than client and account data in banks, personal data controllers are not required by law to take specific measures against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal data. The data controllers will be held liable according to the average man standard if their acts or omissions cause the processing, loss, destruction or damage to such personal data and this in turn results in damage being caused to the data subject.

BREACH NOTIFICATION

There is no mandatory legal requirement in the Egyptian law to report data security breaches or losses to the authorities or to data subjects.

ENFORCEMENT

As a general rule, civil liability may be raised in connection with violations against the individuals’ right to privacy. The prejudiced data subject should establish to the competent court the unlawful act, the damage occurred to them and the causation relationship between the unlawful act and the damage. Compensation is calculated on an ‘actual damages’ basis and is not punitive. Moral damages are also compensated.
Civil liability for data privacy infringement has not been frequently claimed before Egyptian courts.

**ELECTRONIC MARKETING**

Egyptian law does not have any specific provisions which regulate Electronic Marketing.

**ONLINE PRIVACY**

The Egyptian Constitution issued in 2014 provides that internet security is considered an essential part of the economic institution and national security and that the state is responsible for taking any required measures to maintain said security as regulated by the law. However, Egyptian law does not have any specific provisions which regulate online privacy.

There are number of draft legislations that are expected to be promulgated by Parliament in the coming period on state surveillance and the transfer and processing of data, including (i) draft law regarding the combat of the electronic and information crimes; and (ii) draft law regarding cyber security.

Also, please note that the Egyptian Computer Emergency Response Team, which is affiliated to the Ministry of Communication and Information Technology, has been established since April 2009 and is responsible for, inter alia, providing support to entities, banking and government sectors to tackle cyber security threats.

Further, Article 64 of the Telecommunication Law no. 10/2003 provides that the services provider or processor of telecommunications services must maintain, at its sole expense, all the technical capability which will allow the armed forces and the national security authorities to perform its competences within the limit of the law, without prejudice to the protection of private life of the individuals. This provision might be interpreted by the authorities to give them the right to have access to or surveillance on the data and information transferred or processed through telecommunication services in Egypt.

**KEY CONTACTS**

**DATA PRIVACY TOOL**

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

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.

In Estonia all derogations / additional requirements to the GDPR will be provided in the new Personal Data Protection Act (PDPA) and the Personal Data Protection Implementation Act (Implementation Act).

The PDPA will replace the current Personal Data Protection Act. The new PDPA is planned to enter into force on 25 May 2018, however, since it is still pending before the Parliament, it is very unlikely that it will in fact be adopted by 25 May 2018. In addition, the Implementation Act, which specifies amendments to a number of Estonian acts with regard to the GDPR, is also planned to enter into force on 25 May 2018. However, this draft has not yet been introduced to the Parliament, the proceedings are still pending in the Government.

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 (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 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). It further specifies the requirements for the head of the DPI.

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.

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 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 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. 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 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. 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 subject’s life and 30 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 60 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:
  - The processing doesn’t require consent
  - More than 30 (if underaged – 60) years have passed from the data subject’s death
  - 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 and the fact of death.

- 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 and only on condition that the party providing this information 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 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 sufficient public interest exists and such processing is done according to the principles of journalistic ethics. Such publicising 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 for the purposes of scientific or historical research purposes or statistical purposes – 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-pseudonymisation or other measure of changing non-identifiable personal data to identifiable personal data is only permissible for further research or statistical purposes. The processor must name the person, who has access to the data that enables de-pseudonymisation.

The processing of personal data without data subject’s consent in a form that the data subject is identifiable is only permissible when:
  - Pseudonymisation would seriously hinder achieving the purposes of data processing
  - 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 fulfilment 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 or statistic purposes 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 - 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.
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).

The PDPA 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.

Further, with regard to administrative supervision, the DPI is, if the precepts it issued are not fulfilled, entitled to turn to a superior agency, person or body of the processor of personal data for organisation of supervisory control or commencement of disciplinary proceedings against an official. Upon failure to comply with a precept of the DPI, DPI may impose a penalty payment pursuant to the procedure provided for in the Substitutive Enforcement and Penalty Payment Act. The upper limit for a penalty payment is 20,000,000 euros or up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

In addition to the administrative supervision the DPI may also impose fines (in misdemeanour 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.

The PDPA also specifies the term for review of complaints, i.e. the DPI shall settle a complaint within thirty days after the date of filing the complaint with the Data Protection Inspectorate. In order to additionally clarify certain circumstances this term may be extended by up to sixty days. If cooperation with other relevant supervisory agencies is required, then the term is extended by a reasonable period necessary to receive the opinion from the other agency.

**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, a change which is currently forecast for Spring 2019. 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 (e.g. ‘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 (e.g. 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, then 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
T +372 6 400 900
kaupo.lepasepp@sorainen.com

Mihkel Miidla
Senior Associate, Head of Technology & Data Protection
T +372 6 400 959
mihkel.miidla@sorainen.com

DATA PRIVACY TOOL

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

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 Finnish Government has issued a draft proposal for the general national GDPR implementation Act, i.e the Data Protection Act (HE 9/2018 vp, available in Finnish and in Swedish. Unfortunately, Government draft proposals are not usually available in English, only the finalized Acts that has been passed through the Parliament. The original goal was and still is to have the new Act effective on 25th May 2018.

The new Personal Data Act would repeal the current general Personal Data Act (1999/523) and the Act on Data Protection Board and Data Protection Authority (1994/389).

The Act for Information and Communications Services (2014/917, ‘Information Society Code’) and The Act on Protecting Privacy in Working Life (2004/759, ‘Laki yksityisyyden suojasta työelämässä’) shall still be in force unchangeable. However, the upcoming ePrivacy-regulation shall probably lead to changes to these Acts.

Government draft proposal HE 9/2018 vp for new general legislation i.e Data Protection Act to implement GDPR has been submitted into a normal national legislative process on 1 March 2018, where different Committees of the Parliament (Committee for Constitutional Law (always) and Law Committee (always) will issue their statements on the draft proposal to the Administration Committee after having organized various hearings for different experts and interest groups. The Administration Committee will also have hearings and issue a final committee report on the matter to the Parliament plenary session.
Subsequently, the draft proposal will be submitted to a vote in the plenary session of the Parliament and it will either pass or be rejected (highly unlikely at this point).

As per today 10th May 2018, the Committee for Constitutional Law and Law Committee has ceased the hearings and should provide a statement to the Administration Committee during the following days. It remains, however, to be seen whether the new Data Protection Act will become effective on 25th May 2018, since the legislative work is still in progress.

The purpose of the new national general Personal Data Act is to: a) regulate nationally any issue that is mandatory under GDPR and b) use at least some of the national leeway provided by GDPR.

Please bear in mind that Finland also has a lot of special national legislation concerning data protection which can be divided into two main categories:

1. Independent acts and regulations that concern purely data protection issues:
   a. Person registers that are meaningful for the society (e.g. population information registers, student registers and different public administration registers concerning various sectors)

2. Acts that contain some sections related to personal data (e.g. sections on the disclosure, confidentiality, processed data types and data retention periods)

The Ministry of Justice has placed a working group with a mandate to give proposals and notifications regarding the use of national leeway under GDPR (the new Data Protection Act is mostly based on this report “Ministry of Justice reports and statements, 35/2017”) which can be found here in Finnish.

The above-mentioned working group has also provided a final statement (“Ministry of Justice reports and statements, 8/2018”) which can be found here in Finnish. It entails a general review the special national legislation in order to identify Acts and regulations that are not in compliance with GDPR and to identify areas in which special national legislation should be added/amended/repealed.

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.

There is a possibility that Finland shall somehow use the national leeway provided in GDPR 4(1) article sub-section 7 related to the specific criteria for the controller’s nomination, but it cannot be done in general national implementation legislation, i.e. the Data Protection Act but rather in special national legislation. However, nothing concrete has surfaced as per today.

Please note, however, that there are few instances in the national special legislation in which the controller has been designated in advance: Act on Electronic Prescriptions section 18 §: The Finnish Social Insurance Institution is the controller for the recipe centre and the recipe archive: Act on Electronic Processing of Client Information in Social Welfare and Healthcare section 14 a §: The Finnish Social Insurance Institution is the controller of the national patient data management system.

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.

Contact details remain the same.

In accordance with the draft proposal of the new Data Protection Act chapter 3 section 8 and 9 §:

The independent Supervisory Authority will (still) be the Data Protection Ombudsman (in Finnish “Tietosuojavalvottomuus”) and the Office of the Ombudsman for Data Protection (in Finnish “Tietosuojavalvototon virasto”) contains at least one Assistance Data Protection Ombudsman as well as various data protection experts and secretaries as public servants. The Data Protection Ombudsman shall nominate the public servants himself.

The independency will be guaranteed by an obligation to give a detailed account of the engagements under section 8 a § of the Finnish Public Servant Act (1994/750). This obligation concerns the Data Protection Ombudsman and Assistance Data Protection Ombudsman (chapter 3 section 13 §).

The division of labour between the Data Protection Ombudsman and the Assistance Data Protection Ombudsman shall be governed by the Rules of Procedure of the Office of the Ombudsman for Data Protection approved by the Data Protection Ombudsman, the Assistance Data Protection Ombudsman shall the same jurisdiction as the Data Protection Ombudsman while conducting his duties. (chapter 3 section 16 §).

The Data Protection Ombudsman shall be nominated by the Council of State for a term of 5 years. The Ombudsman or
the Assistance Ombudsman may not hold another post during the term. The formal requirement for these positions is a higher law degree and have the ability to conduct international assignments. (chapter 3 sections 10 and 11 §).

The Office of the Ombudsman for Data Protection shall contain an Expert Committee (president, vice president, 3 normal members, each will have a deputy member). The Committee shall be nominated by the Council of State for a term of 3 years. The president and vice president must hold a higher law degree. (chapter 3 section 12 §).

Duties of the Data Protection Ombudsman:

- Shall accredit the certification bodies under GDPR 43 article (chapter 3 section 14 §)
- provide the annual report under GDPR 59 article only to the Parliament and the Government (chapter 3 section 14 §).
- Shall represent Finland at the European Data Protection Board (chapter 3 section 14 §).

Duties of the Expert Committee:

- To provide statements upon the request by the Data Protection Ombudsman on significant questions relating to the application of legislation concerning processing of personal data.

The Committee may, under its own discretion, hear

3. party experts relating to its duties. The secretary of the Committee shall be a rapporteur of the Office of the Ombudsman for Data Protection (chapter 3 section 17 §).

The Data Protection Ombudsman audit rights and the right to obtain information:

- In addition to GDPR 58(1) article, The Data Protection Ombudsman shall be entitled to receive, free of charge, all the necessary information required for the performance of his duties regardless of the Confidentiality Requirement in chapter 6 section 35 §. (chapter 3 section 18 §).
- Audits conducted in a space used for permanent private housing are only permissible if it is necessary for untangling the issues relating to the subject of the audit and there is a grounded and specified reason to suspect that the rules relating the processing of personal data have been violated in a way that may be attributable to administrative fines or a crime stipulated under the Finnish Criminal Code.(chapter 3 section 18 §
- The Data Protection Ombudsman may use 3.party experts while conducting an audit under his jurisdiction. The 3.party expert shall act under the legislation concerning criminal public liability.(chapter 3 section 19 §).

Executive Assistance

- The Data Protection Ombudsman shall be entitled to receive executive assistance from the police while conducting his duties. (chapter 3 section 20 §).

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 draft proposal of the Data Protection Act does not contain any provisions related to registration, and the old requirements under the current Personal Data Act shall be repealed when the new Data Protection Act becomes effective.

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.

Pursuant to GDPR 37(4) article, there are currently two (2) special national Acts that stipulate mandatory DPO’s (i.e Act on Electronic Processing of Client Information in Social Welfare and Healthcare, 2007/159 and Act on Electronic Prescriptions, 2007/61). However, due to GDPR 37(1) sub-section a) every functional unit of the public social welfare and healthcare sector as well as the Finnish Social Insurance Institution (KELA) would have the obligation to nominate a DPO anyways, but the obligation also applies to Pharmacies under the Act on Electronic Prescriptions.

The DPO shall be bound by the general confidentiality requirement stipulated under section 35 § of the new proposed Data Protection Act pursuant to GDPR 38(5) article. The new draft proposal does not entail further sections on 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):

Pursuant to GDPR 37(4) article, there are currently two (2) special national Acts that stipulate mandatory DPO’s (i.e Act on Electronic Processing of Client Information in Social Welfare and Healthcare, 2007/159 and Act on Electronic Prescriptions, 2007/61). However, due to GDPR 37(1) sub-section a) every functional unit of the public social welfare and healthcare sector as well as the Finnish Social Insurance Institution (KELA) would have the obligation to nominate a DPO anyways, but the obligation also applies to Pharmacies under the Act on Electronic Prescriptions.

The DPO shall be bound by the general confidentiality requirement stipulated under section 35 § of the new proposed Data Protection Act pursuant to GDPR 38(5) article. The new draft proposal does not entail further sections on DPO.
• 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 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 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 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. 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.

1. The draft proposal of the Data Protection Act entails a section (4 §) that specifies GDPR 6(1) subsection e).
   Under this section the processing is lawful if:
   a. it relates to a person’s status, position or tasks in the public sector, economic life or the 3. sector and the purpose of the processing rests on public interest grounds in accordance with the principle of proportionality,
   b. processing is necessary for scientific or historical research or statistical purposes and rests on public interest grounds in accordance with the principle of proportionality,
   c. the processing of research material, cultural heritage material and any description information thereof for archiving purposes is necessary on public interests grounds and complies with the principle of proportionality.
   d. the processing is necessary for the operation of Authorities relating to public interest grounds and complies with the principle of proportionality.

2. The draft proposal of the Data Protection Act entails a section (6.1 §) that specifies the national leeway provided in GDPR article 9(2) subsections b), g), h), i), j). These include:
   a. processing of personal data of the insured or claimant within the operation of Insurance Companies in order to settle the Insurance Company’s liability
   b. processing of trade union membership information to comply with the Controller’s obligations in the field of employment law
   c. processing of health and medical data in connection to operation of Healthcare Service Provider
   d. processing of health and medical data in connection to operation of Social Welfare Service Provides
   e. processing of genetic and health data related to antidoping-work and sports of the disabled, when processing is necessary in order to enable antidoping-work or sports of the disabled
   f. processing relates to scientific or historical research or statistics
   g. processing of research and cultural heritage material for non-profit archiving purposes, excluding genetic data

For the purpose of respecting the essence of the right to data protection and the provision of suitable and specific measures to safeguard the fundamental rights and interests of data subject, The draft proposal of the Data Protection Act entails a section (6.2 §) relating to suitable and specific measures:

- measures that enable to verify by whom the personal data has been stored, altered or transferred
- measures to enhance the competence of those who process personal data
- the nomination of DPO under GDPR 37(1) sub-section c).
- pseudonymization of personal data
- encryption of personal data
- Internal measures of the controller and processor to prevent access to personal data
- process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measure for ensuring the security of processing
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services in fault situations
- performing a DPIA under GDPR 35 article
- specific rules of procedure to ensure compliance with the GDPR and the Data Protection Act concerning data transfers or the processing of personal data for purposes other than the original purpose
other technical and organisational measures

The draft proposal of the Data Protection Act entails a section 7 § that specifies the national leeway provided in GDPR article 10:

a. processing personal data relating to criminal convictions and offences is allowed where the processing is necessary for the establishment, exercise, defence and deciding legal claims
b. processing relates to:
   ○ processing of personal data of the insured or claimant within the operation of Insurance Companies in order to settle the Insurance Company’s liability
   ○ processing is necessary for the fulfilment of controller’s direct obligation under the law
   ○ processing relates to scientific or historical research or statistics

- The above-mentioned Data Protection Act section (6.2 §) on suitable and specific measures also applies to this section 7 §.

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.
The draft proposal of the Data Protection Act is silent on the matters relating to transfers of personal data, i.e. Finland has decided not to use the marginal national leeway provided in GDPR 46 and 49 articles as per now.

Note: The current national general Personal Data Act (which will be repealed by the Data Protection Act) does, however, entails an obligation to notify the international transfer to the Data Protection Authority (“Tietosuojavaltuutettu”) in certain circumstances.

**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.

Apart from the above-mentioned section (6.2 §) of the draft proposal of the Data Protection Act relating to suitable and specific measures, the new Data Protection Act does not cover any direct additional requirements for processing security in the meaning of GDPR article 32.

However, the new draft proposal of the Data Protection Act does entail indirect sections concerning security in general, such as section 35 § on Confidentiality Requirement and the amendment of the Finnish Criminal Code (1889/39) chapter 38 section 9 introducing a new “data protection crime” punishable by fines or max. 1 year of imprisonment. This data protection crime is not overlapping with the administrative sanctions under GDPR. The prosecutor must also consult the Data Protection Ombudsman before filing a charge for data protection crime.

**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.

As per now, Finland has opted not to use the national leeway provided in GDPR article 34 in the draft proposal of the Data Protection Act.

However, the national special legislation entails some data breach notification obligations. For instance, a TeleCom company is under the Finnish Information Society Code (2014/917) sections 274-275 § obliged to inform Finnish Communications Regulatory Authority (FICORA), the subscribers and users without undue delay of any significant data breach that prevents or significantly interferes communication services. In addition, the Act Strong Electronic Identification and Electronic Signatures (2009/617) section 16 § stipulates that The identification service provider shall notify, without any undue delay, service providers using its services, identification device holders and the Finnish Communications Regulatory Authority 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).

Note: the national Data Protection Board under the current Personal Data Act will cease to exist and will be replaced by an Expert Committee that has smaller jurisdiction. It only provides statements upon the request from the Data Protection Ombudsman for significant questions related to data processing.

Penalty payment

• The Data Protection Ombudsman may issue a penalty payment as an intensifier of any decision taken under GDPR 58(2) article subsections c)-g) and j) or based on the Ombudsman's right to receive, free of charge, all the necessary information required for the performance of his duties regardless of the Confidentiality Requirement in chapter 6 section 35 §. (chapter 3 section 18 §). The issuing and convicting a penalty payment shall be governed by the Act on Penalty Payment (1900/1113).

Appeal

• The decision of the Data Protection Ombudsman is eligible for appeal to Administrative Court as stipulated in the Act on Administration of Administrative Law (1996/586). (chapter 4 section 23 §).

• The decision of the Administrative Court is eligible for appeal only if the Supreme Administrative Court grants a leave to appeal. The Data Protection Ombudsman shall also have the right for appeal to the Supreme Administrative Court. (chapter 4 section 23 §).

• Any decision of the Data Protection Ombudsman (other than one concerning administrative fines) may entail a decree stating that the decision must be obeyed regardless of any appeal process, unless the appellate authority rule otherwise. (chapter 4 section 23 §).

Commission decisions

• If the Data Protection Ombudsman deems necessary to, concerning a pending issue, settle whether the EU commissions adequacy decision under GDPR article 45 is in accordance with the GDPR, The Ombudsman may
file a petition to the Helsinki Administrative Court. The decision of the Helsinki Administrative Court may be appealed, if the Supreme Administrative Court grants a leave to appeal. (chapter 4 section 24 §)

Administrative Fines (chapter 4 section 25 §)
- An administrative fine in accordance with GDPR 83 article can be issued for violations of GDPR 10 article pursuant to GDPR 83(5) and this (Data Protection) Act
- Administrative fines cannot be issued to the Office of the President of the Republic, State Authorities, state-owned businesses/state-owned companies, local authorities, independent institutions under public law or Parliament offices.
- Administrative fines cannot be issued after 10 years has passed since the offence or neglect has occurred
- The Enforcement of the Administrative Fines shall be governed by the Act on Enforcement of Fines (2002/672) Penal Provisions (chapter 4 section 26 §)
- The penalty for Data Protection Crime (completely new section that shall be incorporated to the Finnish Criminal Code due to the draft proposal of the Data Protection Act) will be governed by chapter 38 section 9 § of the Criminal Code.
- The penalty for Message Interception and Aggravated Message Interception shall (still) be governed by chapter 38 section 3 and 4 § of the Criminal Code.
- The penalty for Computer Break-In and Aggravated Computer Break-In shall (still) be governed by chapter 38 sections 8 and 8 a § of the Criminal Code.
- The penalty for the breach of the Confidentiality Requirement under sections 35 § and 36 § (“protection of the “whistleblower”) of this Data Protection Act shall be governed by chapter 38 sections 1 and 2 § of the Criminal Code (secrecy offence and secrecy violation)
- The Prosecutor shall be obliged to hear the Data Protection Ombudsman before pressing charges for the crimes mentioned above. The Court shall also be obliged to reserve the Data Protection Ombudsman an opportunity to be heard

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, a change which is currently forecast for Spring 2019. 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 Information Society Code regulates direct marketing by electronic means in Finland. The Data Protection Ombudsman is the supervising authority also in compliance issues with the Information Society Code’s 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 forbid 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 unless they have specifically forbidden it. As with natural persons, legal persons must also be able to easily and at no charge forbid 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 (firstname.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 recognised 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 Act will also apply. This means that the data subject may prohibit the use of his/her personal data for advertising or marketing purposes, and that the personal data may only be collected into a data file in accordance with the provisions of the Act.

**ONLINE PRIVACY**

The Information Society Code 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 consent can be given via web browser or other applicable settings. 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.

**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 value added service provided 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 value added service provider or the communications provider at any time.

**KEY CONTACTS**

**Markus Oksanen**
Partner
T +358 9 4176 0431
markus.oksanen@dlapiper.com

**DATA PRIVACY TOOL**

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

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.

**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 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. 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 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.

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:

- 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 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, a change which is currently forecast for Spring 2019. 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

- 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 authorised 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, eg 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 only if the subscriber/user has expressly consented after having received such 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.

In December 2013 the CNIL issued updated recommendations for cookies that are more flexible than the CNIL’s prior position. The CNIL considers that certain cookies are not covered by the Law (e.g. cookies used to constitute a ‘basket’ on an e-commerce platform, session ID cookies, authentication cookies and certain analytics cookies).

Regarding consent, the CNIL has specified that consent must be:

- freely given (i.e. in circumstances where the user has a choice to refuse consent)
- specific (i.e. relate to a specific cookie associated with a clearly defined purpose), and
- informed (i.e. the user must be given information beforehand, specifying the cookie’s purpose as well as the possibility to revoke consent).

The CNIL regards the following consent collection mechanisms as compliant:

- a banner on the first webpage visited (of a particular site), which can specify eg that continuing to visit the site constitutes consent to set cookies
- a consent request zone overprinting on the site’s homepage
- boxes to tick when registering for an online service, and
- buttons that activate functionalities of services that set cookies (such as plugins on social networks).

The CNIL considers that the obligation of obtaining the user’s prior consent is incumbent on website publishers, mobile application publishers, advertisers ("règles publicitaires"), social networks, analytics services providers, etc., which must all comply with the Law, whether they deploy or read cookies on their own or a third party website or application.
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.

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 organisation’s level of data protection maturity.
GERMANY

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 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 was officially published on 5 July 2017 and came into force together with the GDPR on 25 May 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.

Find the English version 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 definitions are the same as in Art. 4 GDPR. Beyond that, the BDSG (New) contains further definitions for 'public bodies of the Federation', 'public bodies of the Länder' and 'private bodies' in Sec. 2 BDSG (New).

**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.

Germany does not have one central Data Protection Authority but a number of different Authorities for each of the 16 German states (Länder) that are responsible for making sure that data protection laws and regulations are complied with. In addition the German Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragte für Datenschutz und Informationsfreiheit – ‘BfDI’) is the Data Protection Authority for telecommunication service providers and represents Germany in the European Data Protection Board. To ensure that all the Authorities have the same approach a committee consisting of members of all Authorities has been established – the 'Data Protection Conference' (Datenschutzkonferenz 'DSK'). The coordination mechanism between the German Authorities mirrors the consistency mechanism under the GDPR.

**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 are no registration requirements in Germany.

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 threshold to designate a Data Protection Officer (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 ten persons dealing with the automated processing of personal data, Sec. 38 (1) first sentence 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 10 persons is not reached, Sec. 38 (1) second sentence BDSG regulates in addition to Art. 37 GDPR, that a DPO has to be designated in case the controller or processor undertakes processing subject to a data protection impact assessment pursuant to Art. 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.

Furthermore, a dismissal protection for the DPO is provided in Sec. 38 (2) in conjunction with Sec. 6 (4) BDSG. The dismissal of the data protection officer is only permitted in case there are facts which give the public body just cause to terminate without notice. After the activity as data protection officer has ended, the data protection officer may not be terminated for a year following the end of appointment, unless the public body has just cause to terminate without notice.

Additionally, Sec. 38 (2) in conjunction with Sec. 6 (5) and (6) BDSG stipulates that the data protection officer shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified, unless they are released from this obligation by the data subject. Moreover, the right to refuse to give evidence of a head of a public body or a person employed by such a body also applies for the DPO.

Moreover, the German Authorities require that the DPO speaks the language of the competent Authorities and data subjects, i.e. German, or at least that instant translation is ensured.

**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 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 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. 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.

The BDSG has additional rules regarding processing of special categories of personal data. Contrary to Art. 9 (1) GDPR, processing of such data is permitted by public and private bodies in some cases, see Sec. 22 (1), 23 (3) BDSG. Also, Sec. 23 BDSG (New) 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 (New) provides a special rule for video surveillance of publicly accessible areas, which is not applicable. According to the German DPAs as well as the unanimous opinion in German legal literature the provision is generally not compliant with the GDPR and therefore must not be applied due to the general principle of the primacy of Union law. This is based in the argument that the GDPR does not contain any opening clause for deviating from Art. 6 para. 1 lit. f) GDPR with respect to video surveillance.

Furthermore BDSG provides special rules regarding processing for employment-related purposes in Sec. 26 BDSG. The German legislator has made very broad use of the opening clause in Art. 88 (1) GDPR and has basically established an own employee data protection regime. This new rules reflect the current German employee privacy rules which also has the consequence that a set of case law of the German Federal Labour Court (Bundesarbeitsgericht – ‘BAG’) will apply. In case the processing is conducted for employment-related purposes it is subject to Sec. 26 BDSG only and a recourse to the general legal grounds set out in Article 6 GDPR are blocked. Personal data of employees can only be processed in the
employment context (setting aside some very special cases under the BDSG when it comes to the assessment of the working capacity of the employee and other handling of special categories data as well as exchange of data with the works council) in these cases:

- The processing is necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract (Sec. 26 (1) sentence 1 BDSG) (please note that the BAG interprets the predecessor provision broader than Art. 6 (1) (b) GDPR)

- Employees’ personal data may be processed to detect crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the processing of such data is necessary to investigate the crime 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 (Sec. 26 (1) sentence 2 BDSG)

- The processing is based on a works council agreement which complies with the requirements set out Art. 88 para. 2 GDPR (Sec. 26 (4) BDSG)

- The processing is based on the written employee consent. A derogation from the written form can apply if a different form is appropriate because of special circumstances. This derogation will most likely never apply in practice. Moreover, the utilization of consent as basis for the processing is particularly problematic in Germany as Sec. 26 (2) BDSG stipulates requirements in addition to Art. 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 DPAs 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 (eg private use of company cars or IT equipment, 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 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
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 same applies as in Article 44 et seqq. 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 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 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 organizational measures to ensure that processing complies with Regulation (EU) 2016/679
- 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.
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 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 regulations regarding the breach of notification are mainly identical to Art. 33, 34 GDPR.

Sec. 29 (1) BDSG stipulates in addition to the exception in Art. 34 (3) GDPR, the obligation to inform the data subject of
a personal data breach according to Art. 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 previous, 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 Sec. 43 (3) BDSG, a notification pursuant to Art. 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).
Regarding the enforcement the German Authorities declared that they are of the opinion that the fines will not only be calculated based on the turnover of the specific affected company, but of the entire group of undertakings. However, whether this interpretation of Art. 83 (4), (5) and (6) GDPR in connection with Recital 150 GDPR is correct is currently highly disputed in Germany with solid arguments against this broad interpretation. The enforcement of fines is subject to the Act on Regulatory Offences (Gesetz über Ordnungswidrigkeiten – ‘OWiG’), other sanctions, eg a temporary or definitive limitation or ban on processing, is subject to the rules regarding administrative procedures.

**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, a change which is currently forecast for Spring 2019. 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 BDSG (New) also does not have any specific provisions regarding marketing. The use of electronic communication for the purpose of direct marketing is currently regulated in Art. 13 of the EU Directive 2002/58 which is implemented in Sec. 7 of the German Act Against Unfair Competition (Gesetz gegen den unlauteren Wettbewerb – ‘UWG’) which will remain unaffected by the BDSG and the GDPR, see Art. 95 GDPR. Both provisions will be replaced by Art. 16 of the ePrivacy Regulation (Regulation on Privacy and Electronic Communications). This will likely not change anything regarding marketing via electronic communications in Germany. According to a recent court decision, processing of personal data for the purpose of marketing communication which is in breach of Sec. 7 UWG also constitutes a breach of the GDPR as it does not follow a legitimate purpose (Administrative Court [Verwaltungsgericht] Saarbrueich, decision dated 9 March 2018, case number 1 K 257/17).

For using electronic communication for direct marketing prior consent is necessary (Double-Opt-In process), Art. 16 (1), e-Privacy Regulation, Sec. 7 (2) no. 1, 2 UWG. According to Article 6 (1) lit. 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) and (2) for which specific products and services he/she will receive marketing offers.

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
- authorisation 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 in order 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 have to inform the users immediately, if any faults of data procession systems of the users become known. Furthermore the service provider has to 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 users’ 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 in order to perform the services requested by the user. Otherwise, users must be provided with an opt-out mechanism. For this purpose, information on the use of cookies together with a link on how to adjust browser settings in order to prevent future use is 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.

So far the German Tele-media Act (Telemediengesetz – ‘TMG’) applied for the purposes of online privacy. The Act stems from both data protection law and IT security law. The GDPR replaces all data protection related obligations from the TMG based on the Directive 95/46/EC. Solely the provisions Sec. 13 (1) sentence 2 TMG and Section 13 (7) TMG (which is based on Article 16 EU Directive on security of network and information systems (NIS Directive)) will still apply. As Sec. 13 (1) sentence 2 TMG does not correctly transpose Article 5 (3) Directive 2002/85/EC into German law, the German Authorities are of the opinion that the data protection rules of the BDSG are fully replaced by the GDPR. The German Authorities also have stated that online-tracking and profiling are only admissible with the data subject’s consent. It remains to be seen whether this position will be upheld in court.

Commercial operators of tele-media services, which include website operators (even if services are provided for free), must, in the case of an automated procedure which permits subsequent identification of the recipient of the service and prepares the collection or use of personal data, inform the recipient of the service at the beginning of this procedure (Section 13 (1) sentence 2 TMG). Furthermore, they must take technical and organizational measures in light of ‘state-of-the-art’ technology to prevent security breaches and unauthorized access to their technical systems and to protect personal data (Section 13 (7) TMG).

**KEY CONTACTS**

Verena Grentzenberg  
Of Counsel  
T +49 40 1 88 88 208  
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 organisation’s level of data protection maturity.
DATA PROTECTION LAWS OF THE WORLD

GHANA

LAW

Data Protection Act, 2012 (Act 843) (‘Act’).

DEFINITIONS

Definition personal data

Personal data is defined as:

- data about an individual who can be identified either:
  - from the data, or
  - from the data and other information in the possession of, or likely to come into the possession of the data controller.

Definition sensitive personal data

The Act does not make provision for 'sensitive personal data'. However 'special personal data', is defined as personal data which relates to:

- a child who is under parental control in accordance with the law, or
- the religious or philosophical beliefs, ethnic origin, race, trade union membership, political opinions, health, sexual life or criminal behavior of an individual.

NATIONAL DATA PROTECTION AUTHORITY

Data Protection Commission (‘Commission’)

Room No. 51
First Floor
Ministry of Communications
Ministerial Enclave
P.O. Box CT 7195
Accra
Ghana

Tel: +233 302 631 455

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.

**DATA PROTECTION OFFICERS**

There is an obligation under the Act for data controllers to appoint data protection officers.

**COLLECTION & PROCESSING**

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.

**TRANSFER**

There are no specific provisions in the Act on the transfer of personal data. However, the sale, purchase, knowing or reckless disclosure of personal data or information is prohibited.
A person who 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 person who sells or offers for sale personal data 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 fine and a term of imprisonment.

A penalty unit is equivalent to GHS12 (approximately USD $4.00).

SECURITY

A data controller is required to take steps to secure the integrity of personal data in the possession or control of a person through the adoption of appropriate, reasonable, technical and organisational measures to prevent:

- loss of, damage to, or unauthorised destruction
- unlawful access to or unauthorised processing of personal data.

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 GHS12 (approximately USD $4.00).

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.

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

There are no specific provisions in relation to on-line privacy. However, a data controller is generally required to take necessary steps to secure the integrity of personal data in the possession or control of a person through the adoption of appropriate,
reasonable, technical and organizational measures.

**KEY CONTACTS**

Reindorf Chambers  
www.reindorfchambers.com  

Kizzita Mensah  
T +233 302 225674/ 249564  
kizzita.mensah@reindorfchambers.com

**DATA PRIVACY TOOL**

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

LAW

A territory within the European Union (by virtue of the accession of the United Kingdom on 1 January 1973) Gibraltar implemented the EU data Protection directive 95/46 EC in 2006 with the Data Protection Act 2004 (‘Act’). Enforcement is through the offices of the Data Protection Commissioner (‘DPC’).

DEFINITIONS

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 sensitive personal data

Information about racial or ethnic origin, religious or philosophical beliefs, trade union membership, health or sex life. The definition includes data regarding the commission or 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

Data Protection Commissioner

Gibraltar Regulatory Authority
Suite 603 Europort
Gibraltar

T 200 74636
F 200 72166

info@gra.gi

REGISTRATION

Data controllers who process personal data must notify the Data Protection Commissioner by registering with the Gibraltar Regulatory Authority (‘GRA’) so that their processing of personal data may be registered and made public in the Data Protection Register, unless an exemption applies. Once registered any changes to the processing of personal data will require the Data Protection Register to be updated.

The notification must contain the following information:
• name and address of data controller and any representative

• description of the personal data being processed and the Categories to which they relate

• description of the purpose of the processing

• description of the recipients or categories of recipient to whom data will be sent

• names of any countries outside the EEA to which data is to be transferred to

• an adequate description of the security measures taken that is sufficient to allow a preliminary assessment of those measures, and

• other information reasonably required by the DPC.

DATA PROTECTION OFFICERS

There is no requirement in Gibraltar for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

Data controllers may collect and process personal data when any of the following conditions are met:

• the data subject has unambiguously given his consent

• the processing is necessary for the performance of a contract to which the data subject is a party, or for actions to be carried out at the request of the data subject prior to entering into a contract

• the processing is necessary in order to comply with a legal obligation to which the data controller is subject

• the processing is necessary to prevent:
  ○ injury or other damage to the health of the data subject
  ○ serious loss or damage to his property
  ○ to protect his vital interests where seeking consent is likely to damage those interests

• the processing is necessary for a public purpose, namely:
  ○ for the administration of justice
  ○ for the performance of a statutory function
  ○ for the performance of a function of Government or of a Government Minister
  ○ the processing is necessary for the performance of a public function carried out in the public interest, and
  ○ the processing is necessary for upholding the legitimate interests of the data controller or of a third party to whom the data are supplied, except where the rights of the data subject under the European Convention of Human Rights and the Gibraltar Constitution prevail.

Where sensitive personal data is processed, one of the above conditions must be met plus one of a further list of more stringent conditions.
TRANSFER

Data controllers may transfer personal data out of the EEA if any of the following conditions are met:

- the country to which the data is being transferred ensures an adequate level of protection by reference to statutory parameters
- the data subject consents to the transfer
- the transfer is necessary:
  - to perform a contract between the data subject and the data controller
  - to take steps at the request of the data subject in order to enter into a contract with the data controller
  - for the agreement or performance of a contract between a third party and the data controller at the request of the data subject
  - the transfer of data is required pursuant to an international obligation of Gibraltar; – the transfer is necessary due to a substantial public interest
  - the transfer is necessary to obtain legal advice either in respect of proceedings or to establish or defend a legal right
  - the transfer is necessary to protect the vital interests of the data subject, and
  - the transfer is made as part of personal data stored on a public register.

If none of these conditions are met, data outside of the EEA may still be transferred if:

- it is to a country approved by the EU commission as safe
- it is to a US organisation falling within the Safe Harbour provisions, or
- on terms incorporating the Model Clauses or approved Corporate Binding Rules. Alternatively the data controller can apply to the DPC for specific approval on a case by case basis.

SECURITY

Data controllers must take appropriate technical and organisational measures against accidental or unlawful destruction, loss or alteration of data, or against unauthorised disclosure or access to the information, and generally against all other unlawful forms of processing.

BREACH NOTIFICATION

There is currently no mandatory requirement in the Act to report data security breaches or losses to the DPC or to data subjects. A mandatory requirement will be introduced with the transposition into Gibraltar law of the Amendments to Directive 2002/58/EC (Directive on privacy and electronic communications) introduced by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

ENFORCEMENT

In Gibraltar, the DPC is responsible for the enforcement of the Act. If he becomes aware that the data controller is in breach of the Act, he can initiate proceedings against the data controller.
The ultimate sanction on conviction for an offence is a fine of GBP 4,000 (in the case of summary conviction in the magistrate’s court) or GBP 10,000 (in the case of indictment in the Supreme Court).

**ELECTRONIC MARKETING**

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (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 provides individuals with the right to prevent the processing of their personal data (e.g., a right to ‘opt out’) for direct marketing purposes.

The Communications (PD&P) Regulations 2006 (‘the Regulations’) prohibit the use of automated calling systems without the consent of the recipient and unsolicited emails can only be sent without consent if:

- the contact details have been provided in the course of a sale or negotiations
- the marketing relates to a similar product or services, and
- the recipient was given a means of refusing the use of their contact details for marketing when they were collected.

Direct marketing emails must not disguise or conceal the identity of the sender in contravention of the E-Commerce Act. SMS marketing is also likely to be included within the prohibition on email marketing.

The restrictions on marketing by email only apply in relation to individuals and not where email marketing is sent to corporations.

**ONLINE PRIVACY**

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.

Usual data protection principals of the Act also apply. 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 DPC 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 organisation’s level of data protection maturity.
GREECE

Last modified 17 October 2018

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.

A bill of law (the 'Bill') was published on 20 February 2018 which was submitted to public consultation. It should be noted that such Bill provides for both the legal measures implementing the Regulation 2016/679 (GDPR) in Greece, as well as the integration into the Greek legal order Directive 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. However the Bill has not been enacted yet.

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 supervisory authority is the Greek Data Protection Authority (hereinafter the Authority or the DPA) – under the reservation of Article 65 of the GDPR on the supervisory bodies of courts and public prosecutors.

### Definitions as per article 4 of the GDPR

Such definitions are similar in the Bill, except for the definition of the public sector which substitutes the definition of ‘international organization’:

‘Public sector’ shall mean the national or public authorities, central and regional, independent public services, legal entities of public law, independent and regulatory administrative authorities, the national or public enterprises and organizations, the legal entities of private law belonging to the state or are subsidized from up to 50% of their annual budget at least or their management is defined by this, the local subsidiarity agencies of first and second instance as well as their legal entities and enterprises.

### 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.

Data Protection Authority
1-3 Kifissias Avenue, Athens, 115 23 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 organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

There is no requirement in the Bill to notify / register with the DPA.

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.

Apart from the cases mentioned in Article 37 para. 1 of the GDPR, obligation of appointment of a data protection officer exists for data controllers or data processors which according to the list on all the processing operations issued by the DPA, which due to their nature, scope and/or purpose require regular and systemic monitoring of data subjects on a large scale.

Courts and Public Prosecutors offices are exempted from the obligation to appoint a DPO.

The appointment of the DPO must be made in writing and notified to the DPA.

**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
Data Protection Laws of the World

Greece

230

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 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. 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 personal data

- Collection and processing of personal data for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller in accordance with the law.

- Processing of personal data for purposes different from those they have been collected for is permitted as long as:
  - it is strictly necessary in order to protect the vital interests of the data subject or of another natural person
  - it is strictly necessary for the performance of a task carried out in the public interest
  - it is strictly necessary for the establishment, exercise or defense of legal claims
  - it is necessary for the prevention, investigation, detection, confirmation or prosecution of criminal offences or the execution of criminal penalties
  - it is strictly necessary for national defense purposes

- Processing of personal data in the context of employment from an employer as data controller is allowed as long as:
  - it is necessary for the fulfillment of respective obligations related to the employment contract or deriving from the law or an individual or collective employment contract
  - it is necessary in order to comply with a legal obligation of the data controller
  - it is necessary in order to secure a vital interest of the employee as data subject or of another individual
  - it is necessary in order to fulfill the legal interest of the data controller or another third party, unless the legal interests or the fundamental rights and freedoms of the employee as data subject prevail
In the case that the data collection and processing is based on the consent of employees, such consent shall be written and distinguished from the employment contract. The employee shall have given his free and explicit consent and have the right to deny or withdraw his consent without negative impacts.

- **Processing of special categories of personal data**: is allowed only as long as it is necessary for the exercise of specific rights and the performance of data controller or data subject obligations deriving from the contract of employment law, including obligations regarding employment security and safety, as well as social security law. It shall be carried out by the employer as data controller exclusively either for defined, explicit and legal purposes linked to the employment contract or for purposes deriving from legal provisions. Employees shall be informed beforehand about the processing purposes.

- The employer as data controller shall collect personal data from the data subjects. Collection of data regarding employee or candidate from third parties is allowed only as long as it is necessary for the fulfillment of legal purpose and the employee is informed beforehand about this collection. Personal data processed within the framework of employment relationship shall be appropriate, limited to the extent necessary for certain purposes related to the employment relationship ‘data minimization’.

- **Health data**: shall be collected directly and exclusively from the employees as long as it is absolutely necessary for:
  a) employment assessment for a certain position, b) the fulfillment of employer’s obligations regarding employment security and safety and c) establishment of employees’ rights and social provisions offer. The performance of medical tests and analysis, such as psychological and psychometry tests, is allowed only in certain cases and as long as it is necessary for the specific job position. Processing of employee genetic data is prohibited, unless a legal clause explicitly sets out such procedure or it is necessary for protection of vital interests of the employees or third parties and upon consultation with the supervisory authority.

- The employer as data controller is entitled to process personal data regarding criminal convictions and offences, as well as security measures, as long as it is necessary for the employment assessment of an employee for a certain position or duties within the framework of the employment relationship.

- **Collection and processing of biometric data**: within the framework of the employment relationship is allowed only if it is necessary for the protection of persons and goods.

- **Processing of audiovisual data through CCTV (Article 6 of the GDPR)** in order to protect individuals or / and goods.

This clause covers the systems permanently established in a certain place that function constantly or for a regular period of time and have the ability to perceive or / and transmit audiovisual signals to a limited number of projection screens or/and recording machines. This clause does not apply to the following cases:

- Non data processing activities, such as the functioning of simple access control systems without data recording
- Activities in the course of a purely personal or household activity except for audiovisual processing through a CCTV system established in a private house, if the camera control scope includes public or common-shared spaces.

Personal data shall be retained for no longer than is necessary for the purposes for which it is being processed. It shall be destroyed within 15 days at the latest unless more specific provisions applying to certain categories determine otherwise. In the case that an event relevant with the processing purposes arises, the data controller is allowed to keep the recording containing this specific event in a separate file for a period of 3 months. After this period of time, the data controller may keep the data longer only in exceptional cases of further investigation of the event and under the obligation of informing the Authority about the necessary recording retention period.

- **Collection and processing of personal data through CCTV within the workplace**: is allowed in special and...
exceptional cases, as long as it is justified by the working conditions and scope and it is necessary for the protection of employees’ health and security or working facilities. Such data shall not be used as exclusive criteria for behavior and efficiency assessment of employees.

The employer is obliged to draft a regulation governing the use of communication means and means of electronic processing in workplaces.

- Access to personal data kept for archiving purposes in the public interest is allowed as long as:
  - The data subjects have given their explicit consent
  - The processing is necessary in order to ensure vital interests of data subject or another individual
  - The processing is necessary for the fulfillment of a legal obligation carried out in the public interest in the exercise of official authority assigned to a third party who requests access to personal data
  - The processing is necessary for the establishment, exercise or defense of legal claims
  - The processing is necessary for scientific, historical or statistical purposes

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, 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.

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 the exercise of this right could possibly hinder the fulfillment of archiving purposes in the public interest or the exercise of third parties’ rights.

In derogation from the provisions of Articles 18, 19, 20 and 21 of the GDPR the data subject’s rights are restricted, if these rights could possibly hinder the fulfillment of the specific archiving purposes in the public interest and such restrictions are considered as necessary for the fulfillment of those purposes.

- Processing of personal data for scientific, historical research purposes or statistical purposes is allowed as long as:
  - the data subjects have given their consent
  - the data controller already has such data from previous research and the data subjects have given their consent to further use or use for relevant purposes
  - The personal data derive from public accessible sources
  - The data controller can prove that the processing is necessary for scientific or historical research purposes or statistical purposes and the data subjects rights do not prevail

**Processing sensitive personal data / consent**

**Articles 7, 8, 9, 10 of the GDPR**

- Processing of health data must be based on the explicit and written consent of the data subject.

- Collection and processing of genetic data or / and preventive genetic diagnosis carried out for health and life insurance purposes is prohibited. Such processing is also prohibited for the data subject family members.

- Processing of personal data relating to criminal convictions and offences is permitted, if it is strictly necessary for the purpose of one of the following:
  - Recruitment and assessment for job positions
  - Employment relations under the certain preconditions and guarantees of article 17
  - Archiving in the public interest, scientific or historical research or statistics in accordance with articles 18 and 19
  - Academic, artistic, literary and journalistic expression in the scope of freedom of expression and information
  - Establishment, exercise and defense of legal claims
Processing of personal data relating to criminal convictions and offences is permitted upon the explicit and written consent of the data subject, if it is necessary to take measures requested by the data subject, such as reintegration. Furthermore, the processing of those personal data in the scope of academic, artistic, literary as well as journalistic purposes shall be the adequate, relevant and limited to secure the freedom of expression and the right to information (‘data minimisation’).

Processing of sensitive personal data, as well as those relating to criminal convictions and offences for scientific or historical research purposes or statistical purposes is allowed in the following cases:

- The data subject has given its prior explicit consent. In cases of clinical trials for scientific purposes the provisions of Art. 28-34 of the Regulation 536/2014 are also applicable
- The data controller has access to those data from previous relevant scientific or statistical research activities and the data subjects have given consent to further use
- The data controller is able to prove that the processing is necessary for scientific or historical research purposes or statistical purposes which do not override the rights of the data subjects.

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.
The transfer of personal data is permitted:

- in order to protect the vital interests of the data subject or another natural person
- for substantial public interest reasons and
- for the establishment, exercise or defence of legal claims

after having provided the data subject with information regarding this purpose as well as all the essential information as specified in article 14 of the GDPR.

The transfer of personal data deriving from a CCTV system to third parties is permitted in the following cases:

- after prior explicit consent of the data subject
- in exceptional cases, after justifiable request of a third party, when the data is necessary to be used as evidence for the establishment, exercise or support of legal claims or crimes

The transfer of personal data to courts, public prosecutors and policy authorities upon request, in the exercise of their legal obligations, is not regarded as transfer to third parties.

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 processing of personal data must be confidential. It must be carried out solely and exclusively by persons acting under the authority of the data controller or the processor and upon his instructions.

In order to carry out data processing, the data controller must choose persons with corresponding professional qualifications providing sufficient guarantees in respect of technical expertise and personal integrity to ensure such confidentiality.

The data controller must implement appropriate organizational and technical measures (TOMs) to secure data and protect it against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access as well as any other form of unlawful processing. Such measures must ensure a level of security appropriate to the risks presented by processing and the nature of the data subject to processing.

If the data processing is carried out on behalf of the data controller, by a person not dependent upon him, the relevant assignment must be in writing. Such assignment must provide that the processor carries out such data processing only on
instructions from the data controller and that all other confidentiality obligations must mutatis mutandis be borne by him.

Before a person enters the scope of a CCTV system, the controller must inform in an appropriate and clear way about the CCTV system, the processing purpose, the establishment place, as well as the time for which the personal data will be retained.

**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.

**As provided in Articles 30 and 31 of the GDPR**

In case of a breach of personal data, the data controller is obliged to notify the DPA within 72 hours as of the moment he is aware of such breach. The data processor needs to immediately notify the data controller of any breach he becomes aware.

Specific details must be included in the notification form on the nature of the breach, the categories of the data the repercussions of the breach and whether the data has been transferred to another Member State.

The notification of a personal data breach to the data subject shall not be performed if the data processing relates to one of the following purposes:

- national security
- national defense
- public security
- prevention, investigation or prosecution of criminal convictions and offences, including the protection from and prevention of threats against public security
- important economic or financial state interests including monetary, financial and tax, public health as well as social insurance issues, especially regarding performance of relevant audits
- establishment, exercise or defense of legal claims, and
- the breach notification would be harmful for the fulfilment of those purposes

**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).

**Administrative fines**

The DPA 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.

**Penalties**

As provided by for Article 84 of the GDPR and namely:

- Anyone unlawfully interfering in any way whatsoever with a personal data file or takes note of such data or extracts, alters, affects in a harmful manner, destroys, processes, transfers, discloses, makes accessible to unauthorized persons or permits such persons to take notice of such data or anyone who exploits such data in any way whatsoever, will be punished by imprisonment.

- If the above mentioned actions refer to special categories of data or data relating to criminal prosecutions, security measures as well as criminal convictions, the perpetrator will be punished by imprisonment for a period of at least one year and a fine amounting between 10,000 Euros and 100,000 Euros, unless otherwise subject to more serious sanctions.

- If the perpetrator of the above mentioned actions acts in order to provide himself or someone else with an unlawful asset, cause pecuniary damage or harm someone else, he will be punished by imprisonment for a period of at least three years and a fine amounting between 100,000 Euros and 300,000 Euros, unless otherwise subject to more serious sanctions.

- If the perpetrator has caused a danger for the free function of the democratic regime or the national security through the above mentioned actions, will be punished by incarceration and a fine of between 100,000 Euros and 300,000 Euros.

- Any data protection officer who infringes the confidentiality obligation in the scope of occupational privacy by announcing or revealing facts or information, which it has been aware of through the exercise of its tasks, in order to benefit itself or a third party or harm the controller, the processor, the data subject or a third party, will be published by imprisonment for a period of time of at least 1 year and a fine of between 10,000 Euros and 100,000 Euros, unless otherwise subject to more serious sanctions.

- All the above mentioned actions shall be prosecuted only following the filing of a criminal complaint.

- The felonies fall under the jurisdiction of the Three-Member Felony Court of Appeals.

**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, a change which is currently forecast for Spring 2019. 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 Law 3471/2006 ‘for the protection of personal data and privacy in electronic communications’ (the ’Law’), in combination with the general provisions of the General Data Protection Regulation (Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data).

According to the provisions of article 11 of the Law, data processing for electronic marketing purposes is allowed only with 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.
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 anonymised 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 doubtful 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 anonymised 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.

Traffic data of subscribers or users held by a CSP must be erased or anonymised 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 doubtful 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 anonymised 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 does 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.

**KEY CONTACTS**

*Kyriakides Georgopoulos Law Firm*

www.kglawfirm.gr

Effie Mitsopoulou  
Partner  
T +30 210 817 1540  
e.mitsopoulou@kglawfirm.gr

**DATA PRIVACY TOOL**

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

LAW

The processing of personal data in Guernsey is regulated by the Data Protection (Bailiwick of Guernsey) Law 2001 as amended (the “Law”).

Guernsey has been recognised by the European Commission as providing an adequate level of protection for personal data for the purposes of the Eighth Data Protection Principle (see European Commission Directive 2003/821/EC).

Enforcement of the law is through the Data Protection Commissioner (the "Commissioner"), an independent public official appointed by the States of Guernsey.

In December 2017, the States of Guernsey approved new GDPR-equivalent data protection legislation ("The Data Protection (Bailiwick of Guernsey) Law, 2017") which is anticipated to come into force at the same time as GDPR is enforced in May 2018, subject to obtaining Privy Council approval. In that regard, businesses based in Guernsey or transacting through Guernsey should prepare for the new regime and review their data estate and international transfers, in particular, in readiness for the implementation of both the local law and the extraterritorial reach of GDPR.

Irrespective of whether the new local legislation is approved, the current adequacy decision will remain in force until reviewed by the European Commission.

DEFINITIONS

Definition of personal data

Under the Law, ‘personal data means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Definition of sensitive personal data

’Sensitive personal data’ means personal data consisting of information as to:

- the racial or ethnic origin of the data subject
- his political opinions
- his religious beliefs or other beliefs of a similar nature
- whether he is a member of a labour organisation, such as a trade union
- his physical or mental health or condition
- his sexual life
- the commission or alleged commission by him of any offence, and
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

Data Protection Office
Guernsey Information Centre
North Esplanade
St Peter Port
Guernsey
GY1 2LQ

T: +44 (0) 1481 742074
F: +44 (0) 1481 742077
W: www.dataci.gg

REGISTRATION

Personal data must not (except in limited circumstances) be processed unless the data controller is registered with the Commissioner. Any data controller who wishes to be included in the register must provide a notification to the Commissioner (an online portal is available). Such a notification must specify:

1. the name and address of the data controller
2. the name and address of any nominated representatives
3. a description of the data and the category or categories of data subject to which they relate
4. why the information is processed
5. a description of any recipient or recipients to whom the data controller intends or may wish to disclose the data, and
6. the names, or a description of, any countries or territories outside the Bailiwick of Guernsey to which the data controller directly or indirectly transfers, or intends or may wish directly or indirectly to transfer, the data.

The notification must also contain a general description of the measures to be taken to prevent unauthorised or unlawful processing of, accidental loss or destruction of, or damage to, personal data.

The data controller is required to notify the Commissioner of any changes to the registered details.

DATA PROTECTION OFFICERS

There is no statutory requirement to have a data protection officer. However, where a data controller is not established in the Bailiwick but uses equipment in the Bailiwick for processing the data (otherwise than for the purposes of transit through the Bailiwick), the data controller must nominate a representative who is established in the Bailiwick. If such a representative is nominated, then their name and address forms part of the registrable particulars as detailed in the section above.

COLLECTION & PROCESSING

Data controllers may process personal data when any of the following conditions are met:

- the data subject consents
- 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 data subject’s request with a view to entering into a contract
- the processing is necessary for compliance with the data controller’s legal obligations, other than an obligation imposed by contract
- the processing is necessary in order to protect the vital interests of the data subject, or
- the processing is necessary for the administration of justice, the exercise of a function in the public interest or the exercise of official authority.
Where sensitive personal data is processed one of a further list of more stringent conditions must also be met.

**TRANSFER**

Personal data must not be transferred to a country or territory outside of the Bailiwick of Guernsey 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.

The exceptions to that principle are as follows:

- the data subject has given consent to the transfer
- the transfer is necessary for the performance of a contract between the data subject and the data controller or for the taking of steps at the request of the data subject with a view to his 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 which is entered into at the request of the data subject or is in the interests of the data subject, or is necessary for the performance of such a contract
- the transfer is necessary for reasons of substantial 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
- the transfer is part of personal data on a public register
- the transfer is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects
- the transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of the data subject.

The Commissioner has published a guidance note entitled 'Exporting Data' which sets out the following approved methods of exporting personal data:

- within the EEA without restrictions
- to another country or territory recognised by a European Commission Decision as ensuring adequate protection
- to entities located in the USA and adhering to the Safe Harbor Privacy Principles
- within a multi-national corporation by using Binding Corporate Rules, which are to be agreed between the exporter and the relevant national Data Protection Authority, or
- to non-EU countries, provided that the transfer is made using the approved EU or (more recommended) the International Chamber of Commerce Contractual Clauses, provided always that the Data Protection Principles (as set out in the Law) are complied with.

Following the decision of the Court of Justice of the European Union in Schrems v Data Protection Commissioner (C36214), the US/EU "Safe Harbour" regime is no longer regarded as a valid basis for transferring personal data to the US. Whilst Guernsey is not a member of the EU, it can (and does) adopt measures prescribed by the EU in certain areas such as data protection. Guernsey uses the EU "adequacy" benchmark to assess whether transfers can be validly made to other jurisdictions.

The Safe Harbour regime had been relied upon as a mechanism for the transfer of data to the US, which did not otherwise have "adequate" measures in place to protect personal data. Now that the regime has been abolished, Guernsey businesses are
reviewing their procedures in light of the Schrems decision and following the establishment of Privacy Shield. Whilst the Commissioner has not adopted any formal stance in response to the Schrems decision or indeed in relation to Privacy Shield, she is maintaining a close dialogue with the Channel Islands’ Brussels office and the UK’s Information Commissioner’s Office.

The Commissioner has confirmed that Guernsey’s existing statutory regime will be adhered to and that she retains the power to investigate complaints made to her, including those founded on transfers reliant upon Safe Harbour as a basis for their validity. It is likely that an arrangement such as Privacy Shield (which is endorsed by the EU) will be respected in Guernsey, for those who wish to transfer personal data to the US.

**SECURITY**

Data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data.

Having regard to the state of technological development and the cost of implementing any measures, the measures required must ensure a level of security appropriate to:

1. the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage to, personal data; and
2. the nature of the data to be protected.

Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must:

1. choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and
2. take reasonable steps to ensure compliance with those measures.

**BREACH NOTIFICATION**

There is no mandatory requirement in the law to report data security breaches or losses to the Commissioner or to data subjects.

However, under the European Communities (Implementation of Privacy Directive) (Guernsey) Ordinance 2004, a provider of a public electronic communications service (the ‘service provider’) is required to notify subscribers of a significant risk to the security of the service.

**ENFORCEMENT**

The Commissioner is responsible for the enforcement of the Law.

If the Commissioner is satisfied that a data controller has contravened or is contravening any of the Data Protection Principles, the Commissioner may serve them with a notice (‘Enforcement Notice’) requiring them, to do either or both of the following:

1. to take, or to refrain from taking, such steps as may be specified. or
2. to refrain from processing personal data.

In certain circumstances the Commissioner may serve on the data controller or the data processor a notice requiring the data controller or data processor to provide specified information to him (‘Information Notice’).

The Commissioner may decide to issue an Information Notice as a result of:

1. a request received by or on behalf of any person who is, or believes themselves to be, directly affected by any processing of personal data, or
2. the Commissioner reasonably requires the information for determining whether a data controller has complied or is complying with the Data Protection Principles.
Failure to comply with an Enforcement Notice or Information Notice is a criminal offence and can be punished:

1. on summary conviction, by way of a fine not exceeding £10,000, or
2. on conviction on indictment, by way of an unlimited fine.

The Law also contains provisions for imprisonment and/or an unlimited fine in the event of a person being guilty of an offence of knowingly or recklessly obtaining, or disclosing personal data, without the consent of the data controller.

**ELECTRONIC MARKETING**

Direct marketing by electronic means to individuals and organisations is regulated by the European Communities (Implementation of Privacy) Directive (Guernsey) Ordinance 2004 (the 'Ordinance'). The Law will also likely have an impact, as there is likely to be processing and use of personal data. The Law does not prohibit the use of personal data for the purposes of electronic marketing but provides individuals with the right to prevent the processing of their personal data (ie a right to 'opt out') for direct marketing purposes.

The Ordinance prohibits the use of automated calling systems without the consent of the recipient. 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 implemented by the UK in relation to cookies have not found 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 Ordinance (defined in Electronic Marketing above).

As a matter of good practice, the use of cookies should be identified to web users and they should be allowed to “opt out” of their use if they so wish.

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. 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 where the user/subscriber cannot be identified from that data or for the provision of a value added service with consent.

**KEY CONTACTS**

Carey Olsen
www.careyolsen.com
DATA PRIVACY TOOL

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

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, a Law for Data Privacy Protection and Habeas Data is being discussed in the Honduran Congress. It is expected to be approved during the first congressional session of 2015.

DEFINITIONS

Definition of personal data

‘Public Personal Data’ under the **Law of the Civil Registry** is: ‘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, and
**Definition of sensitive personal data**

‘Sensitive Personal Data’ in the Law for Transparency and for Access to Public Information is defined 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 honour, personal or family privacy, and self-image.’

Other Definitions:

- **Consent**: Written and express authorisation of the person to whom the personal data refers in order to disclose, distribute, commercialise, 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](http://www.rnp.hn)

2. **Institute for the Access to Public Information**
   
   [http://www.iaip.gob.hn](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, and
- In other cases established by law.

TRANSFER

Individuals and/or companies may not transfer, commercialise, 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 the exceptions set forth above.

SECURITY

The Institute for the Access to Public Information has the authority to enforce all Obligated Entities to take necessary security measures for the protection of the personal data they collect and/or use.

The Law 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 Law gives a secrecy status.

BREACH NOTIFICATION

Breach notification is not required.

ENFORCEMENT

The Institute for the Access to Public Information may receive complaints of 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 authorisation.

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 García 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 organisation’s level of data protection maturity.
HONG KONG

Last modified 26 January 2017

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 was significantly amended (notably as regards direct marketing) in 2012/13.

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.

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

12/F, Sunlight Tower
248 Queen’s Road East
Wanchai
Hong Kong

T +852 2827 2827
F +852 2877 7026

http://www.pcpd.org.hk/

The PCPD is responsible for overseeing compliance with the Ordinance.

REGISTRATION
Currently, there is no requirement for the registration of data users in Hong Kong.

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
- organisations with a large database of members (eg 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 finalised (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 final version of the EU’s data protection framework under the forthcoming General Data Protection Regulation no longer containing a data controller registration scheme, it is unclear whether the Hong Kong DURS scheme will now be implemented.

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 to advocate the development of a privacy management programme and encourage data users to appoint or designate a responsible person to oversee the data users’ compliance with the Ordinance. This role may or may not be a full-time job, and 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 may collect personal data from data a 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 right 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.

Separate, 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 purpose); and to keep and make generally available their policies and practices in relation to personal data.

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 his/her personal data was collected:

- that his/her 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 them is under active consideration by the Hong Kong Government, but this process has been delayed while consideration is given to recent developments in cross-border data transfers in the EU. If these restrictions come into force as currently drafted, they will have a significant impact upon outsourcing arrangements, intra group 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).

SECURITY

Data users are required by the Ordinance to take all practicable steps to ensure that personal data is protected against unauthorised 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 unauthorised 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.

BREACH NOTIFICATION

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, as a matter of best practice the PCPD encourages notification to the PCPD, and to data subjects where there would be a risk of harm by not notifying.

ENFORCEMENT

The PCPD is responsible for enforcing the Ordinance. Generally, unless a specific offence 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 to the enforcement notice is a criminal offence, punishable by a fine of...
up to HK$50,000 and imprisonment for up to 2 years, as well as a daily penalty of HKD$1,000 if the offence continues after conviction. In the case of subsequent convictions, additional and more severe penalties apply. There are also certain specific offences 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$1,000,000 and imprisonment of up to 5 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 offence punishable by a fine of up to HK$1,000,000 and imprisonment of up to 5 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.

**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 by the data subject, 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 their direct marketing purposes (eg 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 by the organisation, communicate the individual’s consent to the intended provision in writing.

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 most direct marketing email messages in Hong Kong contain unsubscribe functions, not just the first message.

Hong Kong’s anti-spam framework is set out in the Unsolicited Electronic Messages Ordinance (Cap. 593).

**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.

**KEY CONTACTS**

Scott Thiel  
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group  
T +852 2103 0519  
scott.thiel@dlapiper.com

Carolyn Bigg  
Of Counsel  
T +852 2103 0576  
carolyn.bigg@dlapiper.com

**DATA PRIVACY TOOL**

You may also be interested in our Data Privacy Scorebox to assess your organisation’s level of data protection maturity.
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 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 recently adopted an amendment to the existing Act (the Hungarian Data Protection Law (Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information) basically with two major issues:

- appointment of the Hungarian DPA, and
- a provision for the DPA to give warning instead of imposing fines for first time infringement of data protection rules

The new law is effective as of June 30, 2018.

Another draft law was submitted to the Hungarian Parliament on June 19, 2018. The draft would modify the current Act on Information and would implement the GDPR and the Directive for the Police and Criminal Justice Sector [Directive (EU) 2016/680]. With respect to the GDPR the draft deregulates current provisions and provides institutional and procedural framework for the application of the substantive law laid down in the GDPR (however, it does not relate to any sectorial laws).

The proposal is being discussed by the Parliament in normal (not expedited) schedule.
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.

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 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. 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 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.

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, a change which is currently forecast for Spring 2019. 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 (e.g. 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 authorised 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, public-opinion polling and market research shall be subject to the prior consent of the subscriber.

**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 defence), 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 authorised 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 authorisation 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 competent Hungarian Authorities have not issued any guidance in respect of the interpretation of ‘consent’ and how this consent should be obtained in practice. General practice is that consent can be obtained via browser settings, however, as mentioned so far this has not been confirmed by the opinion or the guidance of the Authorities yet.

---

**KEY CONTACTS**

Csaba Vari  
Senior Associate  
csaba.vari@dlapiper.com
DATA PRIVACY TOOL

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

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 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 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 (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 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
e-mail: postur@personuvernd.is
www.personuvernd.is

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.

According to Article 31 of the DPA, controllers need to consult with and obtain prior authorisation from the supervisory authority in relation to processing by a controller for the performance of a task carried out in the public interest, including processing in relation to social protection and public health. 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.

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.

**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 .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 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. 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.

**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
- 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.

**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 defence
- 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
- 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.

**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:

- 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 subjects.
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.

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.

Regarding the security of the processing and notification of a personal data breach, Articles 32 and 33 of the GDPR are implemented in the DPA without alterations in Article 27.

The Icelandic Data Protection Authority has issued guidelines for notifications of security breaches which are based on the instructions of the Article 29 Working Party on security breaches and has provided a form for notification purposes.
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.
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 organisation, can lead to daily fines until necessary improvements have been made. Fines can amount up to ISK 200,000 (approximately 1,600 euros) for each day that passes without the Data Protection Authority’s instructions being observed.

Breaches of the DPA can lead to fines from ISK 100,000 (approximately 800 euros) to 1.2 billion ISK (approximately 9,600 euros) (in relation to Article 83(4) of the GDPR) and ISK 100,000 to ISK 2.4 billion (approximately 19,280 euros) (in relation to Articles 83(5)-83(6) of the GDPR), cf. Article 46 of the DPA.

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, a change which is currently forecast for Spring 2019. 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 81/2003 the use of electronic communications systems, including for email and other direct marketing, is only allowed if a subscriber has given prior 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
There are no provisions in Icelandic legislation that specifically deal with the use of cookies or location data. However, location data and IP addresses are considered personal data under the Data Protection Act.

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 unless one of the listed conditions is met, in most instances the data subject must consent to the processing of such data.

**KEY CONTACTS**

LOGOS Legal Services  
www.logoslegalservices.com

Hjördís Halldórsdóttir  
Partner  
T +354 5 400 300  
hjordis@logos.is

Áslaug Björgvinsdóttir  
Partner  
T +354 5 400 300  
aslaug@logos.is

**DATA PRIVACY TOOL**

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

LAW

There is no specific legislation on privacy and data protection in India. However, the Information Technology Act, 2000 (the ‘Act’) contains specific provisions intended to protect electronic data (including non-electronic records or information that have been, are currently or are intended to be processed electronically).

India’s IT Ministry adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules). The Privacy Rules, which took effect in 2011, require corporate entities collecting, processing and storing personal data, including sensitive personal information to comply with certain procedures. It distinguishes both ‘personal information’ and ‘sensitive personal information’, as defined below.

In August 2011, India’s Ministry of Communications and Information issued a ‘Press Note’ Technology (Clarification on the Privacy Rules), which provided that any Indian outsourcing service provider/organisation providing services relating to collection, storage, dealing or handling of sensitive personal information or personal information under contractual obligation with any legal entity located within or outside India is subject to collection and disclosure of information requirements, including the consent requirements discussed below, provided that they do not have direct contact with the data subjects (providers of information) when providing their services.

DEFINITIONS

Definition of personal data

The Privacy Rules define the term ‘personal information’ as any information that relates to a natural person, which either directly or indirectly, in combination with other information that is available or likely to be available to a corporate entity, is capable of identifying such person.

Definition of sensitive personal data

The Privacy Rules define ‘sensitive personal data or information’ to include the following information relating to:

- password

- financial information eg bank account/credit or debit card or other payment instrument details

- physical, physiological and mental health condition

- sexual orientation

- medical records and history
Biometric information

Any detail relating to the above clauses as provided to a corporate entity for providing services, and

Any of the information received under the above clauses for storing or processing under lawful contract or otherwise.

Biometrics means the technologies that measure and analyse human body characteristics, such as ‘fingerprints’, ‘eye retinas and irises’, ‘voice patterns’, ‘facial patterns’, ‘hand measurements’ and ‘DNA’ for authentication purposes.

However, any information that is freely available in the public domain is exempt from the above definition.

NATIONAL DATA PROTECTION AUTHORITY

No such authority exists.

REGISTRATION

No requirements.

DATA PROTECTION OFFICERS

Every corporate entity collecting sensitive personal information must appoint a Grievance Officer to address complaints relating to the processing of such information, and to respond to data subject access and correction requests in an expeditious manner but within one month from the date of receipt of grievance.

There is no specific requirement that the data protection officer must be a citizen of or resident of India, nor are they any specific enforcement actions or penalties associated with not appointing a data protection officer correctly. However, appointment of a data protection officer is part of the statutory due diligence process and it is thus imperative that such an officer should be appointed.

COLLECTION & PROCESSING

Under the Act, if a corporate 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 compliance with the Privacy Rules, and its negligence causes wrongful loss or wrongful gain to any person, the corporate entity shall be liable for damages to the person(s) affected.

The Privacy Rules state that any corporate entity or any person acting on its behalf, which is collecting sensitive personal information, must obtain written consent (through letter, email or fax) from the providers of that information. However, the August 2011 ‘Press Note’ issued by the IT Ministry clarifies that consent may be given by any mode of electronic communication.

The Privacy Rules also mandate that any corporate entity (or any person, who on behalf of such entity) collects, receives, possess, stores, deals or handles information, shall provide a privacy policy that discloses its practices regarding the handling and disclosure of personal information including sensitive personal information and ensure that the policy is available for view, including on the website of the corporate entity (or the person acting on its behalf). Specifically, the corporate entity must ensure that the person to whom the information relates is notified of the following at the time of collection of sensitive personal information or other personal information:

- the fact that the information is being collected
- the purpose for which the information is being collected
- the intended recipients of the information, and
* the name and address of the agency that is collecting the information and the agency that will retain the information.

Further, sensitive personal information may only be collected for a lawful purpose connected with a function or purpose of the corporate entity and only if such collection is considered necessary for that purpose. The corporate entity must also ensure that it does not retain the sensitive personal information for longer than it is required, and should also ensure that the same is being used for the purpose for which it was collected.

A corporate entity or any person acting on its behalf is obligated to enable the providers of information to review the information they had so provided and also to ensure that any personal information or sensitive personal information that is found to be inaccurate or deficient is corrected upon request. Further, the provider of information has to be provided a right to opt out (i.e., he/she will be able to withdraw his/her consent) even after consent has been provided. However, the corporate entity will not be held responsible for the authenticity of the personal information or sensitive personal information given by the provider of information to such corporate entity or any other person acting on its behalf.

**TRANSFER**

The data collector must obtain the consent of the provider of the information for any transfer of sensitive personal information to any other corporate entity or person in India, or in any other country that ensures the same level of data protection as provided for under the Privacy Rules. However, consent is not necessary for the transfer, if it is required for the performance of a lawful contract between the corporate entity (or any person acting on its behalf) and the provider of information or as otherwise specified in the Act.

A corporate entity may not transfer any sensitive personal information to another person or entity that does not maintain the same level of data protection as required in the Act.

The contract regulating the data transfer should contain adequate indemnity provisions for a third party breach, should clearly specify the end purposes of the data processing (including who has access to such data) and should specify a mode of transfer that is adequately secured and safe.

Further, under the Act, it is an offence for any person who has pursuant to a contract gained access to any material containing personal information to disclose that information without the consent of the person concerned, and with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain.

Thus, contracts should also specifically include provisions:

- entitling the data collector to distinguish between ‘personal information’ and ‘sensitive personal information’ that it wishes to collect/process
- representing that the consent of the person(s) concerned has been obtained for collection and disclosure of personal information or sensitive personal information, and
- outlining the liability of the third party.

**SECURITY**

A corporate entity possessing, dealing or handling any sensitive personal information in a computer resource which it owns, controls or operates is required to implement and maintain reasonable security practices and procedures to secure the sensitive personal information. The reasonable security practices and procedures may be specified in an agreement between the parties.

Further, the Privacy Rules provide that in the absence of such agreement ‘reasonable security practices and procedures’ to be adopted by any corporate entity to secure sensitive personal information are procedures that comply with the IS/ISO/IEC 27001 standard or with the codes of best practices for data protection as approved by the Federal Government. Presently, no such codes of best practices have been approved by the Federal Government.

**BREACH NOTIFICATION**
The Government of India has established and authorised the Indian Computer Emergency Response Team (Cert-In), to collect, analyse and disseminate information on cyber incidents, provide forecast and alerts of cyber security incidents, provide emergency measures for handling cyber security 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) impose mandatory notification requirements on service providers, intermediaries, data centres and corporate entities, upon the occurrence of certain ‘cyber security incidents’.

Cyber security incidents have been defined to mean any real or suspected adverse events, in relation to cyber security, that violate any explicitly or implicitly applicable security policy, resulting in:

- unauthorised access, denial or disruption of service
- unauthorised use of a computer resource for processing or storage of information
- changes to data, information without authorisation.

The occurrence of the following types of cyber security incidents, trigger the notification requirements under the Cert-In Rules:

- Targeted scanning/probing of critical networks/systems
- Compromise of critical information/system
- Unauthorized access of IT system/data
- Defacement of websites or intrusion into website & unauthorized changes such as inserting malicious codes, links to external websites
- Malicious code attacks such as spreading virus, worm/Trojan/Botnets/Spyware
- Attacks on servers such as Database, Mail and DNS & Network devises such as Routers
- Identity theft, Spoofing and phishing attacks
- Denial of service (DoS) & Distributed Denial of service (DDoS) attacks
- Attacks on critical infrastructure, SCADA systems and wireless networks
- Attacks on Application such as E-governance and E-commerce etc.

Upon the occurrence of any of the aforementioned events, companies are required to notify the Cert-In within reasonable time, so as to leave scope for appropriate action by the authorities. However, it is important to follow ‘breach notice obligations’, which would depend upon the “place of occurrence of such breaches”, and whether or not Indian customers have been targeted. The format and procedure for reporting of cyber security incidents have been provided by Cert-In on its official website.

**ENFORCEMENT**

Civil penalties of up to EUR 694,450 for failure to protect data including sensitive personal information may be imposed by an Adjudicating Officer; damages in a civil suit may exceed this amount.

Criminal penalties of up to 3 years imprisonment or a fine up to EUR 6,950, or both for unlawful disclosure of information.

**ELECTRONIC MARKETING**

The Act does not refer to electronic marketing directly. However, dishonestly receiving date, computer database or software is an offence.

The Privacy Rules also provide the right to "opt out" of email marketing, and the company’s privacy policy must address marketing
and information collection practices. Further, Do Not Call (DNC) Registry is effectively implemented by the Telecom Regulatory Authority of India (TRAI). Tele-marketing 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, it is advisable that user consent is obtained by inserting appropriate disclaimers.

However, the IT Act contains both civil and a criminal offences for a variety of computer crimes:

- any person who introduces or causes to be introduced any computer contaminant into any computer, computer system or computer network may be fined up to EUR 694,450 (by an Adjudicating Officer); damages in a civil suit may exceed this amount. 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 programmes 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, and
- any person, who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, is subject to a prison term of up to 3 years and fine up to EUR 1,390.

**KEY CONTACTS**

Vakul Corporate Advisory Pvt. Ltd

**Vakul Sharma**  
Managing Partner  
T +91 11 47025460  
vakul@vakulcorp.com

**Seema Sharma**  
Senior Partner  
T +91 11 47025460  
seema@vakulcorp.com

**DATA PRIVACY TOOL**

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

Last modified 24 January 2018

LAW

Specific Regulations

In Indonesia, as of the date of this publication there is no general law on data protection. However, there are certain regulations concerning the use of electronic data. The primary sources of the management of electronic information and transactions are 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 (“EIT Law Amendment”), Government Regulation No. 82 of 2012 regarding Provisions of Electronic systems and Transactions (“Reg. 82”) and its implementing regulation, Minister of Communications & Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System (the “MOCI Regulation”).

However, a new draft Bill on the Protection of Private Personal Data (the “Bill”) is being discussed and to this date it has not been issued. Although the exact date remains uncertain and the Bill is still to be considered by the House of Representatives, if passed, this will become Indonesia’s first comprehensive law to specifically deal with the issue of data privacy.

In addition to the provisions under EIT Law, Reg. 82 and MOCI Regulation, there are also a series of regulations which also cover certain provisions which may relate to data protection, such as:

Telecommunications Sector

Article 40 of Law No. 36 of 1999 regarding Telecommunications (‘Telecommunications Law’) provides that any person is prohibited from any kinds of tapping on information transmitted through any kinds of telecommunications network. Furthermore, Article 42 of the Telecommunications Law stipulates that any telecommunications services operator has to keep confidential any information transmitted and/or received by telecommunications service subscriber through telecommunications networks and/or telecommunications services provided by the relevant operator.
Public Information Sector

Article 6 of Law No. 14 of 2008 regarding Disclosure of Public Information provides that information relating to personal rights may not be disclosed by public bodies. Furthermore, Article 17 of the relevant 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) and evaluation records concerning a person’s capability/recommendation/intellectual, formal/informal education records.

Banking and Capital Markets Sectors

Data privacy in this sector is regulated under Law 7 of 1992 as amended by Law 10 of 1998 on Banking (‘Banking Law’) and Law 8 of 1995 on Capital Markets (‘Capital Markets Law’) respectively. The regulations apply to both individuals and corporate data.

Bank Indonesia’s Regulation No. 9/15/PBI/2007 on the Implementation of Risk Management in the Utilisation of Information Technology by the Bank stipulates that the bank’s customer data transfer (by way of establishing a data centre or a data processing outside Indonesia territory) necessitates prior approval being obtained from Bank Indonesia.

DEFINITIONS

Definition of personal data

Reg. 82 and MOCI Regulation defines Personal Data as: data of an individual, which is stored, maintained and which correctness is preserved and of which its confidentiality is protected (including under the EIT Law and Reg 82).

Definition of sensitive personal data

Currently, there is no specific definition on sensitive personal data under the prevailing laws and regulations.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority for data privacy in general in Indonesia.

For example, the Indonesian Financial Services Authority (‘FSA’) has the authority to act as the regulator of data privacy in the capital markets sector (since 31 December 2012) and with regard to banks’ customer data privacy issues (since 31 December 2013).

However, please note that article 65 of Reg. 82 provides that a business enactor who operates electronic transactions may be certified by a Competence Certification Body (Lembaga Sertifikasi Keandalan) which may be a domestic Indonesian (but currently no such domestic bodies exist) or foreign competence certification body.

REGISTRATION

Minister of Communication and Informatics Regulation No. 36 of 2014 regarding Procedures of Electronic System Provider
Data Protection Laws of the World

Indonesia

Registration ("MOCI Reg 36") differentiates electronic system providers into electronic system provider for public services and electronic system provider for non-public services. An electronic system provider for public services must conduct registration, while an electronic system provider for non-public services may conduct registration, which suggests registration is not mandatory for an electronic system provider for non-public services.

MOCI Reg 36 specifically states that electronic system providers for public services are legal entities related with the government for example state institutions, government agencies, corporations in the form of state-owned enterprises, regional government-owned enterprise, or other legal entities in relation with state’s mission.

Electronic system providers for non-public services are not specifically defined under MOCI Reg 36, but in general other legal entities that are not related with government, such as private corporations, can be classified as electronic system providers for non-public services.

However, the regulators interpret ‘public service’ in regards to electronic system provider pursuant to Government Regulation No. 96 of 2012 regarding Implementation of Law No. 25 of 2009 regarding Public Service ("GR No. 96").

GR No. 96 defines Public Service as an activity or chain of activities in term of fulfilling the service needs in accordance with the law and regulation for every citizen and individual on goods, services, and/or administrative services that are provided by the public service operator. GR No. 96 further defines Public Service Operator as every state operator institution, corporation, independent institution that are formed based on laws for public service activity, and other legal entity that are formed only for the public service activity. Law No. 25 of 2009 regarding Public Services ("Law No. 25"). Article 5 (1) of Law No. 25 provides that the scope of public services includes public goods and services as well as administrative services. Article 5 (2) of Law No. 25 further provides that this includes education, teaching, work and business, housing, communication and information, environment, health, social security, energy, banking, transportation, natural resources, tourism and other stragetic sectors.

In relation to the above, an electronic system provider for non-public services falls under the corporation (non-government related legal entity), providing service for every citizen/individual. Therefore, an electronic system provider for non-public services is also considered as public services pursuant to GR No. 96.

Consequently, all electronic system providers, whether for public services or non-public services, must conduct registration.

Furthermore, Article 4 of Minister of Communications and Informatics Regulation No. 4 of 2016 regarding Management System of Information Protection ("MOCI Reg. No. 4/2016") provides that there are three categories of electronic systems such as: (i) strategic electronic system, which is an electronic system that causes serious impact to the public interest, public services, state governance stability, or state defense and security; (ii) high electronic system, which is an electronic system that causes limited impact to the interest of certain sector and/or territory; and (iii) low electronic system, which is any other electronic system aside from strategic and high electronic systems.

Article 10 of MOCI Reg. No. 4/2016 provides that strategic and high electronic system providers (for public services) must obtain a Certificate of Management System of Information Protection, while low electronic system providers (for public services) may obtain Certificate of Management System of Information Protection.

DATA PROTECTION OFFICERS

There is no requirement in Indonesia for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

EIT Law, Reg. 82 and the MOCI Regulation specifically regulates the obligation to obtain "consent" from the owner of the personal data in the case of data collection, use and processing. Furthermore, Article 7 (1) of MOCI Regulation regulates that in obtaining and collecting Personal Data the electronic system provider must also be limited to the relevant and suitable information in accordance to its purpose and must be conducted accurately. Article 12 (1) of MOCI Regulation also regulates that Personal Data can only be processed and analysed in accordance with the needs of the electronic system provider that have been stated clearly at the time the Personal Data is obtained and collected.
Reg. 82 provide the specific provisions on the obligation for Electronic System Providers to public services to set up a data centre and disaster recovery centre in Indonesia, namely:

- before an Electronic System for public services is implemented, the provider of an Electronic System must register with the Minister of Communication and Information and Technology ("MOCI");

- in providing the provision of an Electronic System, the provider should ensure secrecy, totality and the availability of the Personal Data it manages. The provider should also ensure that the obtaining, the consumption, and usage of Personal Data is based on the consent of the Personal Data owner, except if regulated otherwise [1]. Further the provider should ensure that the usage or disclosure of data is done based on the consent of Personal Data and is in line with the objectives as disclosed to the relevant owner at the time of obtaining the data [2]; and

- the provider of the Electronic System is also obliged to provide audit track records of the Electronic System.

[1] Article 15 (1) (b) of Reg. 82.

[2] Article 15 (1) (c) of Reg. 82.

TRANSFER

Article 22 (2) of Reg. 82 regulates the transfer of data, which provides in any case that in the implementation of an Electronic System and/or Electronic Document aimed to transfer Electronic Information and/or Electronic Document, the Electronic Information and/or Electronic Document must be unique and (the provider shall) explain the control and possession of the Electronic Information and/or Electronic Document.

Article 21 (1) of MOCI Regulation states that displaying, announcing, transferring, broadcasting, and/or opening Personal Data access in the Electronic System can only be conducted:

- By Consent (being defined as a written agreement either manually and/or electronically being given by the owner of Personal Data after obtaining a full explanation regarding the process for acquiring, collecting, processing, analyzing, storing, displaying, announcing, disseminating, storing, displaying, announcing, sending, and disseminating including the confidentiality or non-confidence of the Personal Data), except stipulated otherwise by laws and regulations; and

- After its accuracy and compatibility with the purpose of obtaining and collecting such Personal Data is verified.

Article 22 (1) of the MOCI Regulation states that transferring Personal Data that is managed by an electronic system operator at the government and regional government institution including the public or private sector domiciled in the territory of Indonesia to [parties] outside the territory of Indonesia must:

- Coordinate with the MOCI or the official or institution being authorized for such purpose; and

- Implement the laws and regulations regarding the transboundary exchange of Personal Data.

The implementation of the coordination as stipulated in Article 22 (1) (a) of MOCI Regulation are:

- To report the implementation plan of Personal Data transfer, at least containing the clear name, designated country, recipient subject name, implementation date, and reason/purpose of the transfer;

- To request for advocacy, if needed; and

- To report the activities implementation result.

SECURITY

The obligations of Electronic System Providers are regulated under Reg. 82 and MOCI Regulation, which amongst other things
shall amongst other things:

- 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 implement;
- protect and ensure the privacy and personal data protection of users;
- ensure the appropriate lawful use and disclosure of the personal data;
- provide data centre and disaster recovery centre (for Electronic System Providers for public services);
- provide the audit records on all Provision of Electronic Systems activities;
- 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.

In the telecommunication sector, Article 19 of Minister of Communication and Informatics Regulation No. 26/PER/M.KOMINFO/05/2007 regarding the Security and Utilisation of Internet Protocolbased Telecommunications Network (as amended) ("MR 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 three months.

**BREACH NOTIFICATION**

Article 15 (2) of Reg. 82 provides that the provider of an Electronic System must provide written notification to the owner of personal data, upon its failure to protect the personal data.

Article 20 (3) of Reg. 82 provides that the provider of an Electronic System must make the utmost effort to protect personal data and to immediately report any failure/serious system interference/disturbance to a law enforcement official or the Supervising and Regulatory Authority of the relevant sector.

Article 28 (c) of the MOCI Regulation provides that a written notice to the Personal Data Owner is required if there is a failure in protecting the secrecy of the Personal Data in the Electronic System. The provisions of the notice are as follows:

- must provide reason or cause of the occurrence of the failure in protecting the secrecy of Personal Data;
- can be conducted electronically, if the Personal Data Owner has given Consent for it, at the time of obtaining and collecting his/her Personal Data;
- must ensure that the notice has been received by the Personal Data Owner if the failure contains potential loss to the relevant Personal Data Owner; and
- a written notice is sent to the Personal Data Owner no later than 14 days after the failure is discovered.

**ENFORCEMENT**
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.

The EIT Law and EIT Law Amendment provides criminal penalties ranging from:

- Rp. 600,000,000 fine to Rp. 800,000,000 and/or 6 to 8 years imprisonment for unlawful access;
- Rp. 800,000,000 fine and/or 10 years imprisonment for interception/wiretapping of transmission;
- Rp. 2,000,000,000 to Rp. 5,000,000,000 and/or 8 to 10 years imprisonment for alteration, addition, reduction, transmission, tampering, deletion, moving, hiding Electronic Information and/or Electronic Records.

Failure to comply with Reg. 82 is subject to administrative sanctions (which do not eliminate any civil and criminal liability). These administration sanctions are in the forms of:

- written warning;
- administrative fines;
- temporary dismissal; or
- expulsion from the list of registrations (as required under the regulation).

Failure to comply with MOCI Regulations is subject to administrative sanctions in the form of:

- verbal warning;
- written warning;
- temporary dismissal of activities; and/or
- an announcement in the online website.

**Banking Law**

Under Article 47 of the Banking Law, any commissioner, director or employee of a bank or its affiliates who intentionally provides information which has to be kept secret may be sentenced to imprisonment for not less than two years but not more than four years, and fined at least four billion but not more than eight billion Indonesian Rupiah.

**Capital Markets Law**

Under Capital Markets Law, the Financial Services Authority (Previously BAPEPAM LK) is empowered to impose the following administrative sanctions for breaches of the provisions dealing with data protection. The sanctions comprise:

- A written reminder;
- A fine;
- Limitations on business;
- Suspension of business;
- Revocation of business license;
- Cancellation of approval; and
- Cancellation of registration.

**ELECTRONIC MARKETING**

EIT Law and Reg. 82 do not specifically address electronic marketing.

Article 25 of the EIT Law provides that an Internet website, amongst other things, is acknowledged and protected as an Intellectual Property (IP) and consequently, should fall under the ambit of the relevant IP laws, which may in certain cases fall under the Indonesian Copyright Law.

**ONLINE PRIVACY**
There are currently no laws and regulations concerning cookies and location data.

However, if the data collected by cookies or location data is obtained by the unlawful access of another party’s electronic information, this is subject to 6 to 8 years imprisonment and/or a fine of Rp. 600,000,000 to Rp. 800,000,000.

**KEY CONTACTS**

Ivan Almaid Baely & Firmansyah  
www.iab-net.com

**Erwin Purba**  
Partner  
T +62 21 5790 5090  
erwin.purba@iab-net.com

**Robert Hasan**  
Associate  
T +62 21 5790 5090  
robert.hasan@iab-net.com

**DATA PRIVACY TOOL**

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

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.

Irish data protection law underwent a significant overhaul with the introduction of the Data Protection Act 2018 (the 'Act'). The Act implements Directive (EU) 2016/680 (the 'Directive') and gives further effect to Regulation (EU) 2016/679 (the General Data Protection Regulation or the 'GDPR') in the areas in which Member State flexibility is permitted. The Act largely repeals the current Data Protection Acts 1988 and 2003 (the 'DPA') except for the purposes of national security, defence and the international relations of the state.

For contexts falling under the GDPR, the Act may be cited as the Data Protection Act 2018. For contexts involving the security, defence and international relations of the State, the Act and DPA may be cited together as the Data Protection Acts 1988 to 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 contained within the Act are identical to those 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 (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.

Section 10 of the Act establishes a new An Coimisinéir Cosanta Sonraí (or the Data Protection Commission) (the ‘Commission’) and transfers the functions of the current Data Protection Commissioner to the Commission. The Commission will consist of between one and three members, the number of which shall be determined by the Government. These members will be known as Commissioners. In the event that there is more than one Commissioner, one Commissioner will be appointed as a Chairperson. The Chairperson will have the casting vote in the event of a tie.

The contact details of the Data Protection Commission (or An Coimisinéir Cosanta Sonraí) will be as follows:

**Dublin Office:**
21 Fitzwilliam Square, Dublin 2, D02 RD28, Ireland

**Regional Office:**
Canal House, Station Road, Portarlington, R32 AP23 Co. Laois
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 DPA, certain categories of data controller or data processor were required to register with the Data Protection Commissioner, except in a limited number of circumstances. This requirement no longer exists. Therefore a data controller or processor does not have to inform the Commission of their role and does not have to be entered onto a register.

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.

Section 34 of the Act enables the Minister, following consultation with such other Minister of the Government as he or she considers appropriate and the Commission, to make regulations requiring controllers, processors, or associations or other bodies representing categories of controllers or processors to designate a data protection officer.

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 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. 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.

In accordance with the scope given to Member States under the GDPR, the Act permits exceptions to the prohibition on processing personal data and special categories of personal data for purposes other than for which they were collected. These further purposes include processing where necessary: to prevent a threat to national security, defence, or public security; to prevent, detect, investigate, or prosecute criminal offences; and for exercising or performing any right or obligation under employment or social welfare law. The Act also specifies the lawfulness of processing for select purposes including: establishing, exercising or defending legal rights; limited processing of political data in the course of electoral activities in the State; the administration of justice; insurance and pension purposes; preventative and occupational medicine; public health; archiving purposes; and, in certain circumstances, personal data relating to criminal convictions and offences. Under the Act, the digital age of consent in Ireland has been set at age 16 years.

The Act sets out examples of ‘suitable and specific measures’ that may be taken as appropriate to safeguard the fundamental rights and freedoms of data subjects when processing the personal data of data subjects. These measures are already either explicitly or implicitly contained in the GDPR:

- explicit consent
- limitations on access to the personal data undergoing processing within a workplace
- strict time limits for the erasure of personal data and mechanisms to ensure that such limits are observed
- specific targeted training for those involved in processing operations
- having regard to the state of the art, the context, nature, scope and purposes of data processing and the likelihood of risk to, and the severity of any risk to, the rights and freedoms of data subjects:
  - logging mechanisms to permit verification of whether and by whom the personal data have been consulted, altered, disclosed or erased
  - in cases in which it is not mandatory under the Data Protection Regulation, designation of a data
protection officer
  ○ where the processing involves data relating to the health of a data subject, a requirement that the
    processing is undertaken by a health care practitioner, or a person who in the circumstances owes a duty
    of confidentiality to the data subject that is equivalent to that which would exist if that person were a
    health practitioner
  ○ pseudonymisation of the personal data, and
  ○ encryption of the personal data

The Act also sets out that special categories of personal data, identical to those in the GDPR, may be processed subject to
the suitable and specific measures outlined above for select purposes, including: to prevent treats to national security,
defence or public security; to prevent, detect, investigate or prosecute criminal offences; employment and social welfare
law; legal advice and legal proceedings; electoral activities and functions of the Referendum Commission; administration of
justice and performance of conferred functions; for insurance and pension purposes; for reasons of substantial public
interest; for purposes of Article 9(2)(h) GDPR; for public interest in the area of public health; and for archiving in the
public interest, scientific or historical research or statistical purposes.

**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.
The GDPR provides flexibility for Member States to set limits on the transfer of specific categories of personal data to third countries or international organisations. Excluding law enforcement purposes, the Act has not directly set such limits, but provides that the Minister for Justice, following consultation with other Ministers of Government as he or she considers appropriate, and the Commission may make regulations restricting the transfer of categories of personal data to a third country or an international organisation for important reasons of public policy. Any such regulations may be expressed to apply to one or more of:

- a category or categories of personal data
- a third country or class of third countries, or
- an international organisation

Transfers of personal data to third countries or international organisations for law enforcement purposes are dealt with extensively, but this is in pursuance to the Directive, and not 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.

The security measures set out in the Act reflect those set out in 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 build further on the GDPR’s breach notification requirements or procedures.

**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).

Under the Act the enforcement of data protection law in Ireland is the responsibility of the Commission. The Commission will have responsibility for enforcement of domestic matters but may also be responsible for matters which are pan-European. This would be the case where the Commission is selected as the lead supervisory authority under the ‘one-stop-shop’ principal under the GDPR.

The Act significantly increases the Commission’s ability to enforce data protection law by giving it the following powers:

1. to order a controller or processor to comply with data subject requests
2. to order rectification or erasure of personal data or restriction of processing of personal data
3. to order a controller to communicate a personal data breach to data subjects
4. to issue enforcement notices that require a controller or processor to take such steps as the Commission considers necessary and appropriate
5. to require a report on any matter specified in the enforcement notice served on the controller or processor, or require production of any statement, record, or document pursuant to any provision of European or Irish privacy and data protection laws
6. to audit the practices and procedures of a controller or processor
7. to require production of any documents, records, statements or other information within a controller or processor’s control that are relevant to or required for the audit
8. to impose administrative fines in addition to or instead of other enforcement measures.

The final point (8) is highly significant. The Bill provides that the Commission can impose administrative fines of up to €20 million or 4% of global turnover, whichever is higher. In the case that the subject of an administrative fine be a public body that does not act as an undertaking within the meaning of the Competition Act 2002, the administrative fine may not exceed €1,000,000. In comparison to the DPA, the Act greatly enhances the Commission’s ability to enforce compliance by controllers and processors.

**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, a change which is currently forecast for Spring 2019. 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.

Electronic marketing is not directly dealt with by the GDPR and the Act follows suit. In Ireland, electronic marketing is currently governed by the ePrivacy Directive (Directive 2002/58/EC), implemented in Ireland by the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (the ’2011 Regulations’). The proposed new ePrivacy Regulation, currently in draft form, will replace these. The proposed ePrivacy Regulation is intended to be read in light of the GDPR.

**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. The 2011 Regulations expressly refer to the use of browser settings as a means to obtain consent. There is no express requirement for consent to be ‘prior’ to the use of a cookie. 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 the use of cookies 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 (ie 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

Cookie data is not dealt with by the GDPR, and the Act also does not address this topic. Cookie usage is instead dealt with by the 2011 Regulations. The proposed new ePrivacy Regulation, currently in draft form, will replace these. The proposed ePrivacy Regulation is intended to be read in light of the GDPR.

Location Data

Location data is captured by the GDPR within the definition of personal data. The Act does not specify any additional requirements for processing such personal data.
ISRAEL

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.

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:

- 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 non-computerized 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 (eg medical data, criminal records or...
DATA PROTECTION LAWS OF THE WORLD

information about a person’s political or religious beliefs). However, to date, the Schoffman Committee recommendations have not crystallized into binding legislation.

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 POPL, 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 re-obtained 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 alia, 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). Recently, the IPA published Draft Guidelines specifically referring to the use of surveillance cameras in the workplace. The draft 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.
TRANSFER

The transfer of personal data abroad is subject to the Privacy Protection Regulations (Transfer of Data to Databases Abroad), 5761-2001, 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*, 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.

* Following the decision of the ECJ in Case C-362/14 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.

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.
SECURITY

On March 21, 2017, the Constitution, Law, and Justice Committee of the Knesset approved the Data Security Regs, which shall 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.

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.

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, 1-5 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 12th 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 opt-out/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 record-keeping 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.

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 non-identifiable and anonymous information (which cannot be re-identified) 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
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 organisation's level of data protection maturity.
ITALY

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 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.

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.

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 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 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. 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 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.

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, a change which is currently forecast for Spring 2019. 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, or

- the 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. Last December 2017, the Italian Parliament approved a new draft law on telemarketing, which has not yet been published. The new provisions will bring significant changes, including, among 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.

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.

Legislative Decree No. 69/2012 (implementing the Directive 2009/12/EC) amended the Privacy Code provisions relating to marketing and commercial communications by making reference to the ‘contracting party’s and user’s consent’ rather than to the ‘data subject’s consent’, given that the definition of ‘data subject’ has been amended so as to include only natural persons and exclude companies from the application of the Privacy Code, with the exceptions of electronic marketing provisions. Indeed, the Garante clarified that the provisions of the Privacy Code on marketing obligations still apply to companies as well (and not only to natural persons).

ONLINE PRIVACY

The Privacy Code as amended by Legislative Decree No. 69/2012 (implementing the Directive 2009/12/EC) 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.

The Privacy Code states that the Garante may determine certain simplified modalities to provide contracting parties or users with the information notice and to identify the most efficient and practical ways to implement the new obligations on cookies. For this purpose, the Garante has issued a decision on the “simplified information notice and cookie consent” ("Cookie Decision") in force
since June 2015. With the Cookie Decision, the Garante clarifies the distinction between technical and profiling cookies. Technical cookies are cookies required for providing “electronic communications or information society services”; in other words, all cookies required to ensure the running of the site. To this broad category, the Garante associates also the functionality cookies to improve the service provided to the users (e.g. language preferences) and analytics cookies placed by the publisher or the manager of the site (editore o gestore del sito), provided that the power of identification of the data processed is reduced and the third party providing analytics services undertakes not to combine such data with other information it may have. Behavioral or profiling cookies are all cookies that allow a profiling of the user, so as to propose to the same user more tailored advertising. All cookies which do not fall under the technical cookies category are subject to the requirements provided for profiling cookies.

While no prior consent is provided for technical cookies, behavioral cookies require a specific and express consent.

The Garante clarifies the distinction between first and third party cookies, defining as first party cookies all cookies placed by the publisher or the manager of the site, whereas all third party cookies are simply those cookies that are not placed by the first party. In this respect, the Garante acknowledges that the first parties may well not be aware of the existence of third parties placing cookies through the same first parties’ site. Consequently, in collecting the consent also for third parties’ cookies, the first parties are considered as mere “technical intermediary” (intermediari tecnici). All websites with cookies have to provide for a two layer information notice, with a first summarized notice including a link to a second and more complete notice.

The first simplified notice is set through a banner to be placed in the homepage and any landing page and to be devised in a way to create some “discontinuity” with the usage of the site contents. The banner will also contain some basic information, including a mention of any placing of behavioral or third parties cookies, a link to the extended information notice, the mention that it is possible to deny consent, and the indication that the continuation of the usage of the site will imply a cookie acceptance.

Consent has to be provided through “a positive action”, i.e. by removing banner through a click or continuing to read other underlying active pages. It is not possible to simply ignore the banner. The publisher or manager of the site has to keep track of such consent through a (technical) cookie.

The simplified information notice has to link to the more complete information notice, which will include more analytical information, including all information required by the Privacy Code. Such notice has to include also the links to the third parties’ information notices, or other intermediary parties. It should also be specifically mentioned the possibility to object against the usage of cookies also through the browser settings.

**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 organisation’s level of data protection maturity.
JAPAN

LAW
The Act on the Protection of Personal Information ("APPI") regulates privacy protection issues in Japan and the Personal Information Protection Commission (the "PPC"), a central agency acts as a supervisory governmental organization on issues of privacy protection.

The APPI was originally enacted approximately 10 years ago but was recently amended and the amendments came into force on 30 May 2017.

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 Anonymized Information
"Anonymized 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 subject and 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 anonymized 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 Anonymized Information, and the means by which it shares the Anonymized Information.

**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 data to third parties and creation and handling anonymized 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.

Personal Information Protection Commission

Kasumigaseki Common Gate West Tower 32nd Floor, 3-2-1, Kasumigaseki, Chiyoda-ku, Tokyo, 100-0013, Japan

TEL: +81-(0)3-6457-9680

https://www.ppc.go.jp/en/

**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 employees should be assigned to control personal data (eg 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 recognisable 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 Data

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 Data to third party service providers.

Even disclosing the Personal Data within group companies is considered disclosing the Personal Data 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 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 purpose of use includes the provision of such information to third parties and the method of such provision;
- the nature of the personal data being provided to third parties;
- the method by which personal data is provided to third parties;
- the matter that provision of such information to third parties will be stopped upon the request by the data subject; and
- the method for an individual to submit an opt out request to the company.

The APPI does not provide any examples of how best to obtain consent from individuals before sharing Personal Data. Generally, written consent should be obtained whenever possible. When obtaining consent it would be prudent to clearly disclose to the data subject the identity of the third party to whom the Personal Data will be disclosed, the contents of the Personal Data and how the third party will use the provided Personal Data.

The guidelines issued by the PPC provide the following examples as appropriate methods of obtaining the consent for disclosing Personal Data 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 Data is to be used jointly, the business operator handling personal information could, prior to the joint use, notify the data subjects of or publish the following:

- the fact that the Personal Data will be used jointly
- the item of the Personal Data to be disclosed
- the scope of the joint users
- the purpose for which the Personal Data will be used by them, and
- the name of the individual or business operator responsible for the management of the Personal Data.

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 Data has established similarly adequate standards for privacy protection as specified in the enforcement rules of the APPI.

According to the enforcement rules of the APPI, “similarly adequate standards” means that the practices of the business operator handling the Personal Data are at least equal with the requirements for protection of Personal Data under the APPI or that the business operator has obtained recognition based on international frameworks concerning the handling of Personal Data.
According to the guidelines for offshore transfer, one of the examples of an acceptable international framework is the APEC CBPR system. As of yet, no white-listed countries have been specified under the rules by the PPC. The PPC published a circular stating that they are aiming to specify EU countries as white-listed countries by early 2018.

SECURITY

The APPI requires that business operators prevent the leakage of Personal Data. 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 data 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 nondisclosure contracts with employees who have access to Personal Data, protecting machines and devices and developing a framework to respond to instances of leakage.

BREACH NOTIFICATION

It is not legally required to report a data breach incident to the PPC or to notify the relevant data subjects. However, the PPC guidelines recommend that this notification be made and it is the market standard practice to report data breach incidents in Japan. Not doing so and instead having the breach discovered publicly would have a potentially massive negative impact on brand image and reputation in Japan.

In addition, the PPC guidelines suggest that companies (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 and (iii) send a voluntary notice to the data subject of the breach or publish the data breach, if appropriate and necessary.

According to the PPC guidelines, if a factual situation demonstrates that the Personal Data 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 they 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 handling personal information to submit a report, conduct on-site inspection and request or order the business operator handling personal information to take remedial actions. If a business operator handling personal information does not submit the report and materials, or reports false information they will be subject to a fine of up to JPY 300,000. If a business operator handling personal information does not follow an order from the PPC they will be subject to a penalty of imprisonment for up to six months or a fine of up to JPY 300,000.

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 making the disclosure is an entity, the parties subject to this penalty will be the relevant officers, representatives, or managers responsible for the disclosure as well as the entity, which is subject to the fine specified above.

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 internetorder services, a seller is prohibited from sending email or fax advertisements to consumers unless they provide a prior request or consent (ie an optin 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 (eg 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 (eg 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. However, if the information obtained through cookies may identify a certain individual in conjunction with other easily-referenced information (eg member registration) and it is utilised (eg for marketing purposes), such Purpose of Use of information obtained through the use of cookies must be disclosed under the APPI.

KEY CONTACTS

Lawrence G. Carter  
Partner  
T +81 3 4550 2800  
lawrence.carter@dlapiper.com

Keitaro Uzawa  
Associate  
T +81 3 4550 2800  
keitaro.uzawa@dlapiper.com

Brian Caster  
Associate  
T +81 3 4550 2800  
brian.caster@dlapiper.com
DATA PRIVACY TOOL

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

The Data Protection (Jersey) Law 2005 (Law) came into force on 1 December 2005.

Jersey’s data protection legislation has 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).

In January 2018, the States of Jersey was due to consider new GDPR-equivalent data protection legislation (The Data Protection (Jersey) Law, 2018 and the Data Protection Authority (Jersey) Law, 2018) which are anticipated to come into force at the same time as GDPR is enforced in May 2018, subject to obtaining Privy Council approval. In that regard, businesses based in Jersey or transacting through Jersey should prepare for the new regime and review their data estate and international transfers, in particular, in readiness for the implementation of both the local law and the extraterritorial reach of GDPR.

Irrespective of whether new local legislation is adopted, the current adequacy decision will remain in force until reviewed by the European Commission (which will probably occur by 2022 at the latest).

DEFINITIONS

Definition of personal data

‘Personal data’ is defined under the Law as data relating to a living individual who can be identified:

- from the data, or
- from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Definition of sensitive personal data

‘Sensitive Personal Data’ is defined under the Law as personal data relating to:

- the racial or ethnic origin of the data subject
- the political opinions of the data subject
- the data subject’s religious beliefs or other beliefs of a similar nature
- whether the data subject is a member of a trade union
- the data subject’s physical or mental health or condition
• the data subject’s sexual life

• the data subject’s commission, or alleged commission, of any offence, and

• any proceedings for any offence committed, or alleged to have been committed, by the data subject, the disposal of any such proceedings or any sentence of a court in any such proceedings.

NATIONAL DATA PROTECTION AUTHORITY

Office of the Information Commissioner
Brunel House
Old Street
St. Helier
Jersey
JE2 3RG

T: +44 (0)1534 716530
E: enquiries@dataci.org

REGISTRATION

Data controllers who process personal data must inform the Information Commissioner (an online portal is available) of the following:

• the name and address of the data controller (including a Jersey resident representative if the data controller is outside Jersey)

• a description of the personal data being, or to be, processed by or on behalf of the data controller and of the category or categories of data subject to which they relate

• a description of the purpose or purposes for which the data are being or are to be processed

• a description of the recipients (if any) to whom the data controller intends or may wish to disclose the data, and

• the names, or a description, of any countries or territories outside Jersey to which (directly or indirectly) the data controller transfers, or intends or may wish to transfer, the data.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer in Jersey.

COLLECTION & PROCESSING

Data controllers may collect and process personal data when any of the following conditions are met:

• the data subject consents

• the data controller needs to process the data to enter into or carry out a contract to which the data subject is a party

• the processing satisfies the data controller’s legal obligation

• the processing protects the data controller’s vital interests

• the processing is required by an enactment, the Crown or the government

• the processing is required to perform a public function in the public interest, or to administer justice, or
• the data controller has a legitimate reason for the processing, except if the processing would damage the data subject’s rights, freedoms or other legitimate interests.

Where sensitive personal data is processed, one of the above conditions must be met plus one of a further list of additional conditions.

The data controller must provide the data subject with “fair processing information”. This includes the identity of the data controller, the purposes of processing and any other information needed under the circumstances to ensure that the processing is fair.

**TRANSFER**

The Law provides that data controllers may transfer personal data out of the European Economic Area if any of the following conditions are met:

• the data subject consents

• the transfer is essential to a contract to which the data subject is party

• the transfer is needed 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 legally required or essential to an important public interest

• the transfer protects the data subject’s vital interests, or

• the data is public.

Transfers of personal data to jurisdictions outside of the European Economic Area are allowed if the jurisdiction provides ‘adequate protection’ for the security of the data, or if the transfer is covered by ‘standard contractual clauses’ approved by the European Commission. It is likely that Binding Corporate Rules would satisfy the Law.

Following the decision of the Court of Justice of the European Union in Schrems v Data Protection Commissioner (C36214), the US/EU “Safe Harbour” regime is no longer regarded as a valid basis for transferring personal data to the US. Whilst Jersey is not a member of the EU, it can (and does) adopt measures prescribed by the EU in certain areas such as data protection. Jersey uses the EU “adequacy” benchmark to assess whether transfers can be validly made to other jurisdictions.

The Safe Harbour regime had been relied upon as a mechanism for the transfer of data to the US, which did not otherwise have “adequate” measures in place to protect personal data. Now that the regime has been abolished, Jersey businesses are reviewing their procedures. Whilst the Commissioner has not adopted any formal stance in response to the Schrems decision, she is maintaining a close dialogue with the Channel Islands’ Brussels office and the UK’s Information Commissioner’s Office. Whilst awaiting the revised version of the Safe Harbour Privacy Principles, the Commissioner has confirmed that Jersey’s existing statutory regime will be adhered to, confirming that she retains the power to investigate complaints made to her, including those founded on transfers reliant upon Safe Harbour as a basis for their validity.

The Commissioner has confirmed that Jersey existing statutory regime will be adhered to, and that she retains the power to investigate complaints made to her, including those founded on transfers reliant upon Safe Harbour as a basis for their validity. It is likely that an arrangement such as Privacy Shield (which is endorsed by the EU) will be respected in Jersey, for those who wish to transfer personal data to the US. In practice however, we are aware that those using Safe Harbour/Privacy Shield are considering alternative bases for data transfer.

**SECURITY**

Data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data.
BREACH NOTIFICATION

There are no specific duties to inform the Data Protection Commissioner of breaches. However, best practice is likely to be (following the UK) to inform the Data Protection Commissioner of a breach where a significant number of data subjects are affected or where significant harm may (or has already) occurred.

ENFORCEMENT

In Jersey, the Information Commissioner is responsible for the enforcement of the Law. This is a dual role which combines the statutory office of Data Protection Commissioner under the Law with the office of Information Commissioner for the purposes of the Freedom of Information (Jersey) Law 2011.

If the Information Commissioner becomes aware that a data controller is in breach of the Law, an enforcement notice may be issued requiring the data controller to rectify the position.

Failure to comply with an enforcement notice is a criminal offence and can be punished with an unlimited fine.

ELECTRONIC MARKETING

The Law will apply to most electronic marketing.

ONLINE PRIVACY

The 2011 amendments implemented by the UK in relation to cookies have not found their way into Jersey law and there are no immediate plans for this to be done, however the Law will generally apply.

KEY CONTACTS

Carey Olsen
www.careyolsen.com

Huw Thomas
Counsel
T +44 1534 888900
huw.thomas@careyolsen.com

DATA PRIVACY TOOL

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

Last modified 16 October 2018

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 Personal Data Processing Law has been approved by the parliament and came into force on 5 July 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
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 reproduce the definitions of Article 4 of GDPR and generally uses the same terminology than 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.

According to The Personal Data Processing Law the Data State Inspectorate (DSI) will 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
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.

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 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 Processing Law provides no derogation from the requirements of the GDPR regarding data protection officers. The Personal Data Processing Law provides the rules for examining an individual’s knowledge in data protection and obtaining the status of data protection officer. The Personal Data Processing Law allows data controllers and processors to appoint as data protection officer any person who has the qualifications pursuant to the requirements of the GDPR.

As regards the certification procedure, the Personal Data Processing Law provides for a delegation to the Cabinet of Ministers to determine the application procedure, the content and procedure of the qualification examination, the amount of fees and payment procedures for organizing the qualification exam. However, the qualification examination will not be mandatory as it was under the previous Personal Data Protection Law. According to the Personal Data Processing Law, the certification will be voluntary, and a data controller or processor may appoint as data protection officer any qualified person irrespective of certification.

Personal Data Processing Law also provides for a transitional provision stating that the Cabinet of Ministers shall assess the usefulness of the qualification examination, and submit an appropriate assessment to the parliament on the utility of such examination by June 30, 2021.

**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 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. 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.

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.
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 authorised 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, 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.

SECURITY

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.
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 Personal Data Processing Law does not provide any derogations or additional requirements to the GDPR regarding the 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 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 Processing Law does not provide any derogations or additional requirements to the GDPR regarding the 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 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
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. The administrative penalties are not separately provided in the Personal Data Processing Law.

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 (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, a change which is currently forecast for Spring 2019. 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/her contact information (eg e-mail 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/her personal data and the recipient has not previously declared that he or she does not want to be contacted.

With the Amendments of 19 April 2017 the Law on Information Society Services also contains the procedure 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.

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. Moreover, the person whose location data is being processed has the right to revoke his/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 utilising such location data or if the processing of location data is necessary for the 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/

**Kaupo Lepasepp**  
Partner  
T +372 6 400 900  
kaupo.lepasepp@sorainen.com

**Mihkel Miidla**  
Senior Associate, Head of Technology & Data Protection  
T +372 6 400 959  
mihkel.miidla@sorainen.com

**DATA PRIVACY TOOL**

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

LAW

The right to privacy is recognised and protected in the Constitution of the Kingdom of Lesotho.

Lesotho established a Data Protection Commission (“Commission”) in terms of their Data Protection Act (“the Act”). The 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 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; and
- the views or opinions of any other person about the individual.

Definition of sensitive personal data

The Act defines sensitive personal information as:

- genetic data, data related to children, data related to offences, 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; or
- 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 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 defence 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; or
• the information has deliberately been made public by the data subject.

NATIONAL DATA PROTECTION AUTHORITY

Part 2 of the Act provides for the establishment of a Data Protection Commission, an independent and administrative authority established to have oversight and control over this Act and the respective rights of information privacy provided for.

The powers and duties of the Commission are set out in section 8 of the Act.

REGISTRATION

In terms of section 25(5) of the Act, a data controller shall process personal information only upon notification to the Commission.

DATA PROTECTION OFFICERS

The Act at section 58 authorises 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 Act defines processing as an operation or activity or any set of operations, whether or not by automatic means relating to:

• The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
• Dissemination by means of transmission, distribution or making available in any other form; or
• Merging, linking, as well as blocking, degradation, erasure, or destruction, of information.

In terms of section 15(2) of the Act, personal information shall be processed if:

• 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; or
• 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 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;
DATA PROTECTION LAWS OF THE WORLD

- 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; or
- Compliance is not reasonably practicable in the circumstances of the particular case.

TRANSFER

The Act distinguishes between the transfer of personal information to a recipient in a Member State 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 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 shall only be transferred to recipients, other than in Member States of the SADC, or which are not 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 authorised 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

N/A

BREACH NOTIFICATION

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an authorised 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 e-mail to the data subject’s last known e-mail address;
• placed in a prominent position on the website of the party responsible for notification;
• published in the news media; or
• 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 unauthorised 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 Act.

The Act 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

Direct marketing is defined in section 50 as communication by whatever means of any advertising or marketing material which is directed to particular data subjects.

A data subject is entitled any time by notice to a data controller 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 Act which regulate privacy in relation to cookies and location data. These issues may be dealt with in future regulations, which the Act permits the Minister to make on the recommendations of the Commission.

KEY CONTACTS

DLA Piper South Africa

Janine Simpson
Director
DLA Piper
T 0027 (0) 11 282 0797
janine.simpson@dlapiper.com

Lungelo Magubane
Associate
DLA Piper
T 0027 (0) 11 282 0698
lungelo.magubane@dlapiper.com
DATA PRIVACY TOOL

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

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 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 16 July, 2018.

The Data Protection Law replaced the Law on Legal Protection of Personal Data.

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
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 shall mean any activity consisting of offering goods or services and/or asking opinion on the goods or services offered, by post, telephone or other direct means.

Institutions and authorities shall mean 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 (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 addition to the tasks established in the GDPR, the Data Protection Law authorises 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
- in accordance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), to provide assistance to data subjects residing abroad
- 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)
- 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 authorises 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 and (or) privacy are being considered
- invite experts (consultants), to form working groups on examination of processing or protection of personal data, preparation of personal data protection documents, also 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 and/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

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.

Given that the GDPR does not provide for the registration of data processing activities, registries and related systems will 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; 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 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 (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 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
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 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. authorised 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 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 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 and/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 and/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’ behaviour, 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 authorised 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 (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;
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 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 in order for the transfer to be lawful. A substantiated written refusal to issue it within a maximum of 20 working days may also be communicated by the State Data Protection Inspectorate.

**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:

- 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.

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 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 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 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

http://www.dlapiperdataprotection.com
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 offenses, 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 (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, a change which is currently forecast for Spring 2019. 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"). Only direct marketing tailored to natural persons is subject to the requirements of the above mentioned laws. Direct marketing actions that are targeting legal persons (i.e. companies) are not subject to any of these regulations.

General requirements for direct marketing:

- The customer has given his prior consent. Under Lithuanian law, an opt-in principle applies, i.e. the customer should actively express his willingness to receive commercial communication.
- The customer 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 customer (e.g. “By accepting these terms you agree to receive our commercial communication to the e-mail 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 customers have been given a clear, free-of-charge and easily realisable 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 customer has not objected against such use of the data, at the time of each offer.

None direct marketing should be carried out where the contact has requested not to receive unsolicited direct marketing.

**Exemption:** if the company has obtained a telephone number from its customer within the scope of its business transactions legitimately, the company is permitted to use the telephone number for promotional communication if such communication is regarding similar goods or services of the service provider.

Additional requirements under the Advertising Law:

- Direct marketing must be clearly recognisable as a commercial communication;
- The person on behalf of whom this commercial communication is distributed must be clearly identified; and
- 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 to process personal code for direct marketing purposes.

---

**ONLINE PRIVACY**

**Traffic Data**

Traffic Data held by a public electronic communications services provider 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;
- Consent has been given for the retention of the Traffic Data; and
• 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; or
• 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’s technical structure and for cookies used for showing website’s content. Furthermore, 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).

It is required to provide clear and exhaustive information on use of cookies including information about the purposes of cookies related data processing. 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 the consent through web browser settings is not considered appropriate under Lithuanian laws.

Location data

Processing of location data trigger the regulation of personal data processing laws. The data controller must have a legitimate basis for such personal data processing (e.g. 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.
DATA PRIVACY TOOL

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

Draft law n° 7184 establishing the national data protection authority and implementing the GDPR (the "Draft Law"). The Draft Law is currently under discussions through the legislative process and will repeal and replace the law of 2 August 2002 on the protection of individuals as regards the processing of personal data once adopted. Draft law n° 7168 regarding data processing in criminal matters and matters of national security.

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 the Draft Law; definitions provided by the GDPR will 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 (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.

**Commission Nationale pour la Protection des Données (CNPD), 1, Avenue du Rock’n’Roll, L-4361 Esch-sur-Alzette, 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 and the law on data processing in criminal matters and matters of national security (draft law n° 7168 to be enacted).**

### 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.

No specific provisions in the draft laws.

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.

No specific provisions in the draft laws.

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 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. 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.

The Draft Law provides for three specific provisions complementing the GDPR in the matters that were left to the discretion of the Member States.

1. Processing of personal data for the purposes of journalism, university research, art or literature

This processing is not subject to:

- the prohibition set out under article 9 GDPR.
- limitations applicable to processing of personal data relating to criminal convictions and offences (article 10, GDPR):
  - provided that such processing concerns data made publicly available by the data subject; or
  - if the data are connected to the public life of the data subject; or
  - if the data are closely connected to the 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 organisations (chapter V, GDPR).
- the obligation of the data controller to provide particular information to the data subject where personal data are collected from the data subject, as specified under article 13 of the GDPR.
- 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).
- the obligation to provide the data subject with the right of access to his/her personal data. Such right may be exercised only with the assistance of the CNPD and in the presence of the President of the Press Council or his representative.

2. Processing of personal data for the purposes of statistics or scientific or historical research

The rights of the data subject specified under articles 15, 16, 18 and 21 GDPR may be limited provided that such limitations are proportional to the aim pursued and take into consideration the nature of the data and of the processing.

Such limitation of the data subject's rights may only be applied where the data controller puts in place additional appropriate safeguard measures for the rights and freedom of the data subject, such as, in particular:

- the appointment of the Data Protection Officer (DPO).
- performing an analysis of the impact of the contemplated processing on the protection of personal data.
- anonymising the data processed.

3. Processing of sensitive data

The Draft Law confirms that the processing of sensitive data, including health data, may be carried out by the relevant medical bodies and healthcare professionals in the framework of their activities, as well as by research bodies (with appropriate safeguards), social security organisms, insurance companies, pension funds, the Medical and Surgical Mutual Fund and other approved organisms. The lawful transfer of sensitive data between these actors is also facilitated.

**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 specific provisions in the draft laws.

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).

The CNPD may:

- impose administrative fines as provided for in article 83 of the GDPR, including with respect to any legal persons of public law;
- impose on the controller or processor a fine of up to five per cent of its average daily turnover in the previous financial year, respectively during the last financial year closed;
- 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 (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, a change which is currently forecast for Spring 2019. 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 a product or a service, 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.

**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 these data unless they have been 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/her consent, notwithstanding his/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 these data unless they have been 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/her consent thereto, 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 consent of the subscribers or users 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 and free of charge, of temporarily refusing 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/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 user’s consent may be expressed by appropriate browser/application settings.

KEY CONTACTS

Olivier Reisch
Partner
T +352 26 29 04 2017
olivier.reisch@dlapiper.com

Eugene H.C. Tchen
Of Counsel
T +352 26 29 04 25 69
eugene.tchen@dlapiper.com

DATA PRIVACY TOOL

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

Last modified 24 January 2017

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 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/her physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

Pursuant to the Law, ‘sensitive personal data’ can be defined as any personal data revealing political persuasion or philosophical beliefs, political and joint trade unions affiliation, religion, private life and racial or ethnical origin as well as data related to health or sex life, including genetic data.

NATIONAL DATA PROTECTION AUTHORITY

‘Gabinete para a Protecção de Dados Pessoais’, in Portuguese, ‘’, in Chinese, and ‘Office for Personal Data Protection’, in English (‘OPDP’) is the Macau regulatory authority responsible, inter alia, for supervising and coordinating the implementation of the Law.

T: +853 2871 6006
F: +853 2871 6116

www.gpdp.gov.mo

REGISTRATION

The processing of personal data shall be notified to the OPDP by the data processor unless an exemption applies.

For certain data categories (e.g. some sensitive data, data regarding illicit activities or criminal and administrative offences or credit and solvability data) and certain specific personal data processing, prior authorisation from the OPDP is required.

Any variations or changes to the personal data processing determine the amendment of the initial registration.

As for filing requirements, the OPDP provides (official) forms that must be submitted either in Portuguese or Chinese language.
along with, in particular, the following information (if applicable):

1. identification and contact details of the data processor as well as its representatives

2. the personal data processing purpose

3. identification and contact details of any third party carrying out the personal data processing

4. the commencement date of the personal data processing

5. the categories of personal data processed (disclosing whether sensitive data is to be collected as well as data concerning
   the suspicion of illicit activities, criminal and/or administrative offences, as well as data regarding credit and solvability)

6. the legitimacy grounds to process personal data

7. the means and forms available to the data subject for updating his/her personal data

8. any transfer of personal data outside Macau, along with the grounds of and measures to be adopted with the transfer

9. personal data storage time limit

10. interconnection of personal data with third parties, and

11. security measures adopted for the protection of personal data.

DATA PROTECTION OFFICERS

There is no legal requirement to appoint a data protection officer in Macau.

COLLECTION & PROCESSING

Personal data may only be processed if the data subject has given his/her unequivocal consent or if processing is deemed necessary to:

1. the execution of an agreement where the data subject is a party to or in previous diligences for the conclusion of an
   agreement at the request of the data subject

2. the compliance of a legal obligation to which the data processor is subject

3. the protection of vital interests of the data subject if he/she is physically or legally unable of giving his/her consent

4. the performance of a public interest assignment or in the exercise of public authority powers vested in the data processor
   or in a third party to whom the personal data is disclosed, or

5. pursuing a data processor (or a third party to whom the data is disclosed) legitimated interest, provided that the data
   subject interests or rights, liberties and guarantees shall not prevail.

Moreover, the data subject shall be provided with all relevant processing information, including the identification of the data
processor, the personal data processing purpose and the means and forms available to the data subject for accessing, amending
and deleting his/her personal data.

TRANSFER

The transfer of personal data outside Macau can only take place if the recipient country ensures an adequate level of personal data
DATA PROTECTION LAWS OF THE WORLD

Exceptionally, the transfer of personal data outside Macau pursuant to a data subject unequivocal consent is allowed. In such case, the data transfer can be carried out immediately after filing the registration with the OPDP.

SECURITY

The data processor must implement adequate technical and organisational measures to protect the personal data against accidental or illicit 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 illicit forms of processing. Such measures shall 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 related costs with its implementation.

BREACH NOTIFICATION

Under the Law, there is no mandatory requirement for data processors to notify the OPDP or data subjects about any personal data breach in Macau.

ENFORCEMENT

Breaches of the Law are subject to civil liability, administrative and criminal sanctions, including fines and/or imprisonment.

ELECTRONIC MARKETING

Under the Law, data subjects have the right to object, on their request and free of charge, to the processing of their personal data for the purpose of direct marketing and 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 a disclosure or use.

ONLINE PRIVACY

The rules stated in the Law also apply in the online environment.

For example, where a Macau company collects personal data from Macau residents through its website (by cookies, for instance), such Macau company must fulfil all obligations under the Law imposed on data processors, in particular to inform data subjects of the personal data processing purpose and to duly notify the OPDP about the personal data processing, etc.

KEY CONTACTS

LVT Lawyers
www.lvt-lawyers.com

Tang Weng Hang
Partner
T +853 2871 5588
tangwenghang@lvt-lawyers.com

António Lobo Vilela
Partner
T +853 2871 5588
lobovilela@lvt-lawyers.com
DATA PRIVACY TOOL

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

LAW


DEFINITIONS

Definition of personal data

The DP Law defines personal data as any information relating to an identified or identifiable natural entity, where an identifiable entity is an entity whose identity can be especially determined, directly or indirectly, on the basis of his/her personal identification number or on one or a combination of features that are specific for his/her physical, mental, economic, cultural or social identity.

Definition of sensitive personal data

Under the DP Law, sensitive personal data is personal data related to:

- the racial or ethnic origin
- the political views, religious or other beliefs
- membership in a trade union, and
- data relating to the health condition of natural entities, including genetic data, biometric data or data referring to the sexual life.

NATIONAL DATA PROTECTION AUTHORITY

The Macedonian data protection authority is the Directorate for Personal Data Protection (‘DPA’). It was established in 2005 as an independent state agency with competence to oversee the implementation of the DP Law. The DPA’s registered seat is in

Bulevar Goce Delcev 8
Skopje
www.dlzp.mk

REGISTRATION

Any natural or legal entity which intends to collect, process and/or maintain a database containing personal data (‘Database’) in Macedonia is required to notify the DPA prior to the commencement of any such activity. Exceptionally, entities which:

- employ less than 10 employees
intend to process publicly available personal data, or
intend to process personal data of members of non-profit organisations that are established for political, philosophical, religious or trade-union purposes, are excluded from the notification requirements.

The notification requirements mean that entities are required to register both themselves as data controllers and the respective Databases with so-called Central Register of Databases - an electronic register of data controllers and Databases maintained and managed by the DPA. The registration process is carried out on-line by using the DPA’s web application at www.dzlp.mk. A data controller is required to provide all relevant information on particular data processing activities and on its role regarding the same such as: corporate details, purpose of the processing, time period for the retention of processed data, types of the respective data, legal ground for the Database’s establishment, transfer of personal data to other countries, security measures for protection of the respective data’s integrity, etc.

Following the successful registration, the DPA issues a letter to a data controller by which it confirms that the data controller has fulfilled the notification requirements under the DP Law. Any subsequent changes of the details in the registered Databases have to be reported to the DPA within thirty (30) days from the date when such changes took place.

DATA PROTECTION OFFICERS

The DP Law requires data controllers (only those that are subject to the notification requirements set out in the section ‘Registration’ above) to appoint a data protection officer. The data protection officer has an overall responsibility to ensure compliance of the data controller with the DP Law and subordinate regulations, in particular the following:

- to participate in the adoption of all decisions relating to the processing of personal data, as well as the exercise of the rights of the data subjects over their personal data
- to draw up the corporate by-laws for personal data protection, including documents relating to the technical and organizational measures for ensuring confidentiality and protection of personal data
- to monitor the compliance of the data controller with the DP Law and other related regulations, especially in relation to the corporate by-laws for protection of the personal data
- to coordinate the internal procedures and guidelines for the personal data protection, and
- to prepare and deliver a training to the data controller’s employees regarding the personal data protection.

COLLECTION & PROCESSING

The DP Law sets out the main principles for the collection and processing of personal data, which require data controllers to collect and process personal data:

- fairly and lawfully
- for legitimate purposes
- proportionally to the needs for the collection and processing,
- accurately and completely, and
- to ensure that the data is stored in a way which enables the identification of the data subjects.

Data controllers are required to obtain a data subject’s explicit consent for the collection and processing of his/her personal data (including his/her personal identification number and sensitive personal data). This has to be so-called informed consent which means that data controllers have to provide data subjects with all the relevant details about the particular collection and processing of their personal data (such as the processing’s purpose, the data subjects’ rights with respect to the same, retention policy, further transfers, etc). Exceptionally, the DP Law allows data controllers to collect and process personal data without a data subject’s consent (eg for the protection of the life or vital interests of the data subjects, protection of the public interest or the exercise of the data controllers’ legitimate rights (unless this would jeopardize the fundamental rights and freedoms of the data subjects)).
TRANSFER

Transfer of personal data out of Macedonia is allowed only if the third country in question provides an adequate level of personal data protection. The authority to assess whether a third country provides an adequate level of protection and to approve transfers of personal data out of Macedonia is vested with the DPA. However, an assessment and a subsequent approval from the DPA is not required for a transfer of personal data to the countries which are either:

- members of the European Union (‘EU’) or the European Economic Area (‘EEA’), or
- are ‘white-listed’ (were assessed to provide an adequate level of the personal data protection) by the European Commission.

The legal assumption that the EU/EEA and ‘white-listed’ countries provide an adequate level of the personal data protection is enshrined in the DP Law. Moreover, the DP Law completely relies on the European Commission’s assessment of the adequacy of a level of protection in non-EU/EEA countries. Therefore, if any third country is assessed by the EC as a country that does not provide an adequate level of legal protection, the transfer of personal data from Macedonia to such country would not be allowed.

In the above context, a transfer of personal data to a country which is not a member of the EU/EEA or a ‘white-listed’ country is subject to an assessment and approval by the DPA. There is very little practice regarding the approach of the DPA in the process of the respective assessment and approval, nevertheless it is envisaged by the DP Law that the DPA assesses the personal data protection’s adequacy in a third country by especially taking into account:

- the nature of the data
- the purpose and duration of the proposed processing
- governing law in the country where the data is to be transferred, and
- protective measures existing in the respective country.

SECURITY

The DP Law does not require data controllers and processors to implement security measures for the protection of personal data by using a particular technology. However, it does require data controllers and processors to undertake appropriate technical and organizational measures for the protection from accidental or illegal damaging of the personal data, or its accidental loss, change, unauthorized disclosing or access, especially when the processing includes a transmission of the data over a network, and for the protection from any kind of illegal processing.

The implemented technical and organisational measures should be proportional to the risk of the data integrity's breach during the processing and the nature of the data being processed. In this context, the DP Law provides guidance for establishing of three levels of personal data protection by using a combination of technical and organizational measures:

1. basic
2. medium
3. high

Both data controllers and processors are required to adopt internal regulations (ie corporate by-laws) containing a description of the technical and organizational measures for the protection of personal data.

BREACH NOTIFICATION
The DP Law does not require data controllers and processors to report data security breaches to the DPA. Accordingly, the DPA is able to trace data security breaches only if a data subject reports a breach of his/her rights or by performing random inspection of data controllers and processors.

ENFORCEMENT

The DPA has an exclusive duty to oversee the implementation and to enforce the DP Law. It has the authority to monitor data controllers and processors’ compliance with the DP Law by carrying out random inspections or upon receiving a complaint from a data subject.

If the DPA finds that a data controller and/or processor is in breach of the DP Law, depending on the seriousness of the offence, it may order the remedy of the irregularities within a certain period of time or impose a fine. The fines range from EUR 1,000 to EUR 2,000 (per irregularity) for a legal entity and from EUR 350 to EUR 650 for the responsible person at the legal entity. The DPA is also authorized to request from the data controller and/or processor which breached the DP Law to attend a mandatory training on data protection issues organized by the DPA itself. The only available legal remedy against DPA’s decisions for imposing fines on data controllers and/or processors is to initiate an administrative dispute proceeding before the Administrative Court.

Moreover, the Macedonian Criminal Code foresees criminal liability for the misuse of personal data. This criminal offence is punishable with a monetary fine (as determined by the court) or imprisonment for up to one (1) year.

ELECTRONIC MARKETING

The DP Law allows the processing of personal data for the purposes of electronic marketing only if the data subject has explicitly consented to the respective processing provided that the data subject is entitled to withdraw his/her consent at any time free of charge.

ONLINE PRIVACY

There are no specific regulations governing on-line privacy (including cookies). Accordingly, the general data protection rules prescribed by the DP Law apply, to the extent possible, to on-line privacy as well.
DATA PROTECTION LAWS OF THE WORLD

MADAGASCAR

Last modified 24 January 2017

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.

In order to come into effect, the Data Protection Law must be published in the Official Gazette of the Republic of Madagascar. This is expected to occur during the course of this year.

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 others convictions
- trade-union affiliation
- 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.

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) (ie 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 not provide any legal requirement to appoint a data protection officer (délégué à la protection des données à caractère personnel) in Madagascar. However, an entity is exempt from making prior declarations to the CMIL if the entity has appointed a data protection officer ('DPO').

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 controller 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 defence 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  
T +(261) 20 23 25623  
sahondra@madalaw.com

**DATA PRIVACY TOOL**

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

Malaysia’s first comprehensive personal data protection legislation, the Personal Data Protection Act 2010 (PDPA), was passed by the Malaysian Parliament on 2 June 2010 and came into force on 15 November 2013.

DEFINITIONS

Definition of personal data

‘Personal data’ means any information in respect of commercial transactions, which:

- is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose
- is recorded with the intention that it should wholly or partly be processed by means of such equipment, or
- is recorded as part of a relevant filing system or with the intention 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 and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but 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 political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister of Communications and Multimedia (Minister) may determine by order published in the Gazette. Other than the categories of sensitive personal data listed above, the Minister has not ‘gazetted’ any other types of personal data to be sensitive personal data as of 12 January 2018.

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 shall 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 shall not exceed a term of three years, however members can be appointed for two terms in succession.
Decisions of the Commissioner can be appealed against through the Personal Data Protection Appeal Tribunal. These are decisions such as:

- 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, or
- the refusal of the Commissioner to conduct or continue an investigation which 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**
   1. A licensee under the Communications and Multimedia Act 1998
   2. A licensee under the Postal Services Act 2012
2. **Banking and financial institution**
   1. A licensed bank and licensed investment bank under the Financial Services Act 2013
   2. A licensed Islamic bank and licensed international Islamic bank under the Islamic Financial Services Act 2013
   3. A development financial institution under the Development Financial Institution Act 2002
3. **Insurance**
   1. A licensed insurer under the Financial Services Act 2013
   2. A licensed takaful operator under the Islamic Financial Services Act 2013
   3. A licensed international takaful operator under the Islamic Financial Services Act 2013
4. **Health:**
   1. A licensee under the Private Healthcare Facilities and Services Act 1998
   2. 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
   3. A body corporate registered under the Registration of Pharmacists Act 1951
5. **Tourism and hospitalities**
   1. 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
   2. A person who carries on or operates a registered tourist accommodation premises under the Tourism Industry Act 1992
6. **Transportation**
   1. Malaysian Airlines System (MAS)
   2. Air Asia
   3. MAS Wings
   4. Air Asia X
   5. Firefly
   6. Berjaya Air
   7. Malindo Air
   8. Malaysia Airlines Berhad
7. **Education**
   1. A private higher educational institution registered under the Private Higher Educational Institutions Act 1996
   2. A private school or private educational institution registered under the Education Act 1996
8. **Direct selling**
   1. A licensee under the Direct Sales and Anti-Pyramid Scheme Act 1993

9. **Services**
   1. 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
   2. 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
   3. 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:**
   1. A licensed housing developer under the Housing Development (Control and Licensing) Act 1966
   2. A licensed housing developer under the Housing Development (Control and Licensing) Enactment 1978, Sabah
   3. A licensed housing developer under the Housing Developers (Control and Licensing) Ordinance 1993, Sarawak

11. **Utilities**
   1. Tenaga Nasional Berhad
   2. Sabah Electricity Sdn. Bhd
   3. Sarawak Electricity Supply Corporation
   4. SAJ Holding Sdn. Bhd
   5. Air Kelantan Sdn. Bhd
   6. LAKU Management Sdn. Bhd
   7. Perbadanan Bekalan Air Pulau Pinang Sdn. Bhd
   8. Syarikat Bekalan Air Selangor Sdn. Bhd
   9. Syarikat Air Terengganu Sdn. Bhd
   10. Syarikat Air Melaka Sdn. Bhd
   11. Syarikat Air Negeri Sembilan Sdn. Bhd
   12. Syarikat Air Darul Aman Sdn. Bhd
   13. Pengurusan Air Pahang Berhad
   14. Lembaga Air Perak
   15. Lembaga Air Kuching
   16. Lembaga Air Sibu
   17. Pengurusan Air Selangor Sdn. Bhd

12. **Pawnbroker**
   1. A licensee under the Pawnbrokers Act 1972

13. **Moneylender**
   1. A licensee under the Moneylenders Act 1951

Certificates of registration are valid for a period of at least one year (but presently, the Commission grants certificates of registration which are valid for a period of two years), and a data user who fails to renew a certificate of registration and continues to process personal data after the expiry of the certificate of registration commits an offence.

Data users are also required to display their certificate of registration at a conspicuous place at their principle place of business, and a copy of the certificate for each branch, where applicable.

The Commissioner may designate a body as a data user forum in respect of 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 is an offence under the PDPA. As of 12 January 2018, the
Commissioner has published several codes of practice including for the banking and financial sector, the utilities sector and the insurance and Takaful industry in Malaysia.

Therefore, companies may want to consider participating in such data user forums to take part in shaping the codes of practice, as this provides them with an opportunity to influence the codes of practice which companies will ultimately have to comply with.

**DATA PROTECTION OFFICERS**

Currently, there is no requirement for data users to appoint a data protection officer in Malaysia.

**COLLECTION & PROCESSING**

Under the PDPA, subject to certain exceptions, data users are generally required to obtain the consent of data subjects for the processing (which includes collection and disclosure) of their personal data. Where consent is required from a data subject under the age of eighteen, the data user shall obtain consent from the parent, guardian, or person who has parental responsibility on the data subject.

Further, 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.

There are also other obligations imposed on the data user in relation to the processing of personal data, including, for example, requirements to notify the data subjects regarding the purpose for which their personal data are collected.

In terms of disclosure to third parties, in addition to obtaining the consent of the data subject for such disclosure, data users must ensure that they keep and maintain a list of the disclosures to third parties.

On 23 December 2015, the Commissioner published the Personal Data Protection Standard 2015 (Standards), which provides the minimum requirements for processing personal data issued by the Commissioner. Data users must ensure that it takes into account the matters set out in the Standards in the processing of personal data. The Standards include the establishment of standards for the following matters:

- 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, such as where:

- the data subject has given his 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 which, if that place were Malaysia, would contravene the PDP, 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 (Draft Order) to obtain public feedback on the proposed jurisdictions to which personal data from Malaysia may be
transferred. As of 12 January 2018, the Minister has yet to approve the safe harbour jurisdictions. Once approved, a data user may transfer personal data to these safe harbour jurisdictions without having to rely on the data subject’s consent or other prescribed exceptions under the provisions for a restriction of transfer under the PDPA.

SECURITY

Under the PDPA, data users have an obligation to take ‘practical’ steps to protect personal data and in doing so shall develop and implement a security policy. The Commissioner may also from time to time set out security standards which the data user must comply with, and the data user is required to ensure that its data processors also 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, modifications, unauthorized or accidental access or disclosure, alteration or destruction of personal data.

BREACH NOTIFICATION

There is no requirement under the PDPA for data users to notify authorities regarding data protection breaches in Malaysia.

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 personal data system and the data user is required, at all reasonable times, to open the personal data protection system for inspection by the Commissioner or any inspection officer. The Commissioner or the inspection officers may require the production of the following during inspection:

- in relation to general principle, the record of the consent from a data subject maintained in respect of the processing of personal data by the data user
- in relation to notice and choice principle, the record of a written notice issued by the data user to the data subject
- in relation to disclosure principle, the list of disclosure to third parties in respect of personal data that has been or is being processed by him
- in relation to security principle, the security policy developed and implemented by the data user
- in relation to retention principle, the record of compliance in accordance with the retention standard
- in relation to data integrity principle, the record of compliance in accordance with the data integrity standard, and
- such other related information which the Commissioner or any inspection officer deems necessary.

Violation of the PDPA and certain provisions of the Personal Data Protection Regulations 2013 attracts criminal liability. The prescribed penalties include the imposition of fines or a term of 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 defence.

However, 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.

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 personal data for purposes of direct marketing. ‘Direct marketing’ means the communication by whatever means of any advertising or marketing material which is directed to particular individuals.

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

Zaid Ibrahim & Co
www.zicolaw.com/

Sharon Tan
Partner
T +603 20879849
sharon.suyin.tan@zicolaw.com

DATA PRIVACY TOOL

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

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 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 (the 'Act') (Chapter 586 of the Laws of Malta) and the Regulations (at present eleven in number) issued under it. The Act has repealed and replaced the previous Data Protection Act (Chapter 440 of the Laws of Malta).

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 New 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 (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 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 Commission has the function (among others) of generally protecting the individuals' rights to data protection against the violation of their privacy by the processing of their personal data.
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 Act does not contain any obligation for data controllers or data processors to be registered with the Commissioner.

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 derogate or further regulate from the provisions of the GDPR in this regard.
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 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:

- 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 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 reasons of archiving purposes in the public interest. The same abovementioned criteria (1) and (2) above must also 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, shall be 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)
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. This grey area is still subject to local authoritative interpretation. We are not aware of any such interpretations at time of writing.

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.

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.

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 130 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 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 twenty days from the 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 from the filing of the appeal, the Registry of the Tribunal shall:

- serve a copy of the appeal on the Commissioner and request him to file a statement on his decision together with any other information on which such decision was based, within 20 days from the date on which the appeal was served; and
- serve a copy of the appeal on the respondent/s to the appealed decision, and request the respondent/s to 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 €25,000 for each violation and an additional €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 €50,000 for each violation and additionally €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 €1,250 and not more than €50,000 and/or to imprisonment for six months.

**Actions against a controller/processor**

Without prejudice to any other remedy available to him, a person who believes that his rights under the GDPR or this 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/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 ought to 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 (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, a change which is currently forecast for Spring 2019. 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 e-mails) 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/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 he is free to change, alter or withdraw such data at a later date. The personal data which shall be used in the directory must be limited to what is necessary to identify that subscriber and the number allocated to him, unless the subscriber has given his additional consent authorising 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, or
- electronic mail

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 electronic mail 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 electronic mail 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 E-Privacy Regulation would need to be analysed separately.

**ONLINE PRIVACY**

**Cookie Compliance**

Legal Notice 239 of 2011 entitled ‘Processing of Personal Data (Electronic Communications Sector)(Amendment) Regulations 2011’ was brought into force with effect as of 1st January 2013. This Legal Notice amended the regulations thereby implementing into Maltese Law the amendments under Article 2(5) of Directive 2009/136/EC. Having said the above, the local Supervisory Authority (the Commissioner) is yet to issue local guidelines on the way in which the so called ‘cookie clause’ is to be interpreted. We have no information indicating when/if these guidelines may be published. It is worth noting that the Commissioner’s website presently makes reference to the Article 29 Data Protection Working Party Document 02/2013 providing guidance on obtaining consent for cookies (adopted on 2 October 2013).

Although the Bill does not introduce any new legislation in this regard, it is expected that the new GDPR rules on consent will have an effect on the way in which cookies are implemented in Malta.

**Traffic Data**

Under the Electronic Communications 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, shall be erased or made anonymous when it is no longer required for the purpose of transmitting a communication.

Traffic data required for the purposes of subscriber billing or interconnection payments may be retained provided however that the retaining of such data shall only be permissible up to the period during which the bill may be lawfully challenged or payment pursued.

Furthermore, traffic data may be processed where the aim is to market or publicise 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 enquiries
- fraud detection, and
- rendering of value-added services.

The Bill 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 the user or subscriber’s 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, and
- whether the processed data shall be transmitted to a third party for the purpose of providing the value-added service.

A user and/or subscriber may withdraw their consent for the processing of such location data (other than traffic data) at any time.

**Cookie Compliance**

Subsidiary Legislation 586.01 entitled ‘Processing of Personal Data (Electronic Communications Sector) Regulations’ (recently renumbered to Subsidiary Legislation 586.01 from 440.01) amended the regulations thereby implementing into Maltese Law the amendments under Article 2(5) of Directive 2009/136/EC. Having said the above, the local Supervisory Authority (the Commissioner) is yet to issue local guidelines on the way in which the so called ‘cookie clause’ is to be interpreted. We have no information indicating when/if these guidelines may be published. It is worth noting that the Commissioner’s website still makes reference to the Article 29 Data Protection Working Party Document 02/2013 providing guidance on obtaining consent for cookies (adopted on 2 October 2013).

Although the Act does not introduce any new legislation in this regard, it is expected that the new GDPR rules on consent will have an effect on the way in which cookies are implemented in Malta.

**Traffic Data**

Under the Electronic Communications 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, shall be erased or made anonymous when it is no longer required for the purpose of transmitting a communication.

Traffic data required for the purposes of subscriber billing or interconnection payments may be retained provided however that the retaining of such data shall only be permissible up to the period during which the bill may be lawfully challenged or payment pursued.

Furthermore, traffic data may be processed where the aim is to market or publicise 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 enquiries
- fraud detection, and
- 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 of a value-added service.

Prior to obtaining the user or subscriber’s 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, and
- whether the processed data shall be transmitted to a third party for the purpose of providing the value-added service.

A user and/or subscriber may withdraw their 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. Antoine Camilleri**

Partner  
T +356 21 231 345  
antoine.camilleri@mamotcv.com

**Dr. Claude Micallef-Grimaud**

Senior Associate  
T +356 21 231 345  
claude.micallefgrimaud@mamotcv.com

**DATA PRIVACY TOOL**

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

LAW

The Data Protection Act 2004, [Act 13 of 2004], ("Act") was enacted on July 1, 2004 and partially came into force on December 17, 2004 and fully came into operation on February 6, 2009. The Act is largely based on 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.

DEFINITIONS

Definition of personal data

Personal data are data which relate to an individual who can be identified from those data, or data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion.

Definition of sensitive personal data

Sensitive personal data are personal data pertaining to the racial or ethnic origin, political opinion or adherence, religious belief or other belief of a similar nature, membership to a trade union, physical or mental health, sexual preferences or practices, commission or alleged commission of an offence or any proceedings for an offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings of the data subject.

NATIONAL DATA PROTECTION AUTHORITY

Data Protection Office

5th Floor, Happy World House
Corner SSR and Sir William Newton Streets,
Port Louis, Mauritius

Tel: +230 212 22 18
Fax: +230 212 21 74

http://dataprotection.govmu.org/

REGISTRATION

A data controller (an individual or a group of persons who make a decision with regard to the purposes for which and in the manner in which any personal data are, or are to be, processed) as well as a data processor (a person, other than an employee of...
the data controller, who processes the data on behalf of the data controller) must be registered with the Data Protection Office ("DPO"). Registration is a period not exceeding one (1) year and on the expiry of such period, the relevant entry in the Data Protection Register which is kept and maintained by the DPO, is cancelled unless the registration is renewed.

**Application for registration:**

1. a written application for registration is made to the Data Protection Commissioner ("Commissioner").

2. specific particulars must be furnished at the time of the application, depending on whether the application is being made by a data controller or a data processor.

**If the application is being made by a data controller:**

- name and address of the data controller;

- if it has nominated a representative for the purposes of this Act, the name and address of the representative;

- a description of the personal data being, or to be processed by or on behalf of the data controller, and of the category of data subjects, to which the personal data relate;

- a statement as to whether or not he holds, is likely to hold, sensitive personal data;

- a description of the purpose for which the personal data are being or are to be processed;

- a description of any recipient to whom the data controller intends or may wish to disclose the personal data;

- the names, or a description of, any country to which the data controller directly or indirectly transfers, or intends or may wish, directly or indirectly to transfer the data; and

- the class of data subjects, or where practicable the names of data subjects, in respect of which the data controller holds personal data.

A data controller who, knowingly supplies false information for the purposes of an application for registration commits an offence and, on conviction, is liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 2 years.

**If the application is being made by a data processor:**

- name and address of the data processor;
• a description of the personal data being, or to be processed, and the category of data subjects to which the personal data relate;

• the country to which the data controller transfers, or intends to transfer, the personal data; and

• a statement as to whether or not the data processor processes, or intends to process, sensitive personal data; and such other particulars as the Commissioner may require.

A data processor who knowingly supplies false information for the purposes of an application for registration commits an offence and, on conviction, is liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 2 years. At the moment, there is no separate registration for data processors as most of them are also data controllers and are therefore registered as such.

Should a data controller or data processor intend to keep or process personal data or sensitive personal data for 2 or more purposes, an application for separate registration in respect of any of those purposes and entries must be made.

Upon the payment of the prescribed fee, the Commissioner grants an application for registration, unless she reasonably believes that (a) the particulars to be included in the Data Protection Register are insufficient or any other information required by the Commissioner either has not been furnished, or is insufficient (b) appropriate safeguards for the protection of the privacy of the data subjects concerned are not being, or will not continue to be, provided by the data controller, or (c) the person applying for registration is not a fit and proper person.

DATA PROTECTION OFFICERS

The Act does not explicitly require the appointment of a data protection officer. However, the data controller must, at the time of making for registration, specify the name of a person who will supervise the application of the Act within the data controller’s organisation or nominate a representative in relation to the personal data with which the application for registration is concerned.

COLLECTION & PROCESSING

Personal data

Unless an exemption applies, a data 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) is necessary for that purpose.

At the time of collection, the data controller or any person acting on his behalf, must ensure that the individual is aware of certain information, for example (i) the fact that the data is being collected, (ii) the purpose or purposes for which the data is being collected, (iii) the intended recipients of the data, (iv) the name and address of the data controller, (v) whether or not the data collected shall be processed and whether or not the supply of the data by that data subject is voluntary or mandatory, (vi) the consequences if all or part of the requested data is not provided.
It is the duty of the data controller to take all reasonable steps to ensure that personal data within his possession is accurate and up-to-date.

Furthermore, as a general rule, a data controller cannot process the personal data of an individual unless the express consent of the individual has been obtained. There are certain exceptional cases in which personal data can be processed without the express consent of an individual, namely where the processing of personal data is necessary (a) for the performance of a contract to which the individual is a party, (b) in order to take steps required by the individual prior to entering into a contract, (c) in order to protect the vital interests of the individual, (d) for compliance with any legal obligation to which the data controller is subject, (e) for the purpose of making use of a unique identification number to facilitate sharing information and avoid multiple registrations among public sector agencies, (f) for the administration of justice, or (g) in the public interest.

**Sensitive personal data**

As a general rule, the processing of sensitive personal data cannot be processed unless the individual has given his express consent to the processing of the personal data or has made the data public.

However, there are certain exceptions to the general rule, for instance if such processing is:

1. necessary (i) 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 his employment, (ii) in order to protect the vital interests 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, (iii) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld, (iv) for the performance of a contract to which the data subject is a party, (v) in order to take steps required by the data subject prior to entering into a contract, (vi) for compliance with a legal obligation to which the data controller is subject.

2. carried out by any entity or any association which exists for political, philosophical, religious or trade union purposes in the course of its legitimate activities.

3. in respect of the information contained in the personal data made public as a result of steps deliberately taken by the data subject.

4. required by law.

**TRANSFER**

A data controller may only transfer personal data to another country if he has obtained the written authorisation of the Commissioner. However, personal data shall not be transferred to another country unless that country ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data. The adequacy of the level of protection of a country is assessed in light of all the circumstances surrounding the data transfer, having regard to the following: (a) the nature of the data, (b) the purpose and duration of the proposed processing, (c) the country of origin and country of final destination, (d) the rules of law, both general and sectoral, 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.
It is to be noted that the transfer of personal data to another country not ensuring an adequate level of data protection may take place in the following circumstances:

1. the data subject has given his consent to the transfer,

2. the transfer is necessary (i) for the performance of a contract between the data subject and the data controller, or for the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller, (ii) for the conclusion of a contract between the data controller and a person, other than the data subject, which is entered at the request of the data subject, or is in the interest of the data subject, or for the performance of such a contract, (iii) in the public interest, to safeguard public security or national security.

3. the transfer is made on such terms as may be approved by the Commissioner as ensuring the adequate safeguards for the protection of the rights of the data subject.

SECURITY

A data controller has a statutory obligation to take appropriate security and organisational measures for the prevention of unauthorised access to, alteration of, disclosure of, accidental loss, and destruction of the data in his control. Moreover, a data controller should also ensure that the measures provide a level of security appropriate to the harm that might result from the unauthorised access to, alteration of, disclosure of, destruction of the data and the nature of the data concerned. 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 (a) the state of technological development available, (b) the cost of implementing any of the security measures, (c) the special risks that exist in the processing of the data, (d) and the nature of the data being processed.

The Act imposes an obligation on every data controller and data processor to take all reasonable steps to ensure that any person employed by him is aware of and complies with the relevant security measures. If the services of a data processor are retained, the data controller shall choose a data processor providing sufficient guarantees in respect of security and organisational measures.

If the purpose for keeping personal data has lapsed, the data 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 data controller.

BREACH NOTIFICATION

There is no specific provision in the Act which provides for the reporting of data security breaches or losses of data to either the Commissioner or to data subjects. However, in its ‘Guidelines for Handling Privacy Breaches,’ (March, 2010), the DPO encourages organisations to inform the DPO to inform the Commissioner of material breaches so that the DPO is aware of such breaches.

Whilst there is no legal obligation to inform an individual of a data security breach concerning his or her personal data, the Guidelines provides that the organisation must notify the individual of the breach if it is necessary so as to avoid or mitigate harm to the individual.

ENFORCEMENT

The enforcement authority for the Act is, in the first place, the Commissioner. If the Commissioner is of the opinion that a data controller or a data processor has contravened, is contravening or is about to contravene the Act, the Commissioner may serve an enforcement notice on the data controller or the data processor, as the case may be, requiring him to take such steps within such time as may be specified in the notice.
The enforcement notice must:

1. specify the provision of the Act which has been, is being or is likely to be contravened;

2. specify the measures that shall be taken to remedy or eliminate the matter, as the case may be, which makes it likely that a contravention will arise;

3. specify a time limit which shall not be less than 21 days within which those measures shall be implemented; and

4. state that there is a right of appeal.

A person who, without reasonable excuse, fails or refuses to comply with an enforcement notice commits an offence, and, on conviction, is liable to a fine not exceeding 50,000 rupees and to imprisonment for a term not exceeding 2 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. Upon being satisfied, the Judge in Chambers issues a preservation order specifying a period which is not more than 90 days during which the order shall remain in force. However, the time period may be extended beyond 90 days upon application by the Commissioner.

The Commissioner may carry out periodical audits of the systems of data controllers or data processors to ensure compliance with data protection principles laid down in the Act. Where the Commissioner is of the opinion that the processing or transfer of data by a data controller or data processor entails specific risks to the privacy rights of data subjects, she may inspect and assess the security measures taken prior to the beginning of the processing or transfer. Moreover, at any reasonable time during working hours, the Commissioner may carry out further inspection and assessment of the security measures imposed on a data controller or data processor.

For the purposes of gathering information or for the proper conduct of any investigation concerning compliance with the Act, the Commissioner may seek the assistance of such persons or authorities, as she thinks fit and that person or authority may do such things as are reasonably necessary to assist the Commissioner in the performance of the Commissioner’s functions. Upon the completion of an investigation which reveals that an offence has been committed under the Act or any regulations under the Act, the Commissioner shall refer the matter to the police.

The Commissioner may delegate any of her investigating and enforcement powers conferred upon her by the Act to any officer of her office and to any police officer designated by her for that purpose.

**Electronic Marketing**

The use of personal data for the purposes of electronic marketing is not prohibited by the Act. However, at any time, an individual may by way of written notice request a data controller to either stop or not to begin the processing of personal data in respect of which he is a data subject, for the purposes of direct marketing (i.e. the communication of any advertising or marketing material which is directed to any particular individual).
Upon receiving such a request, the data controller must as soon as reasonably practicable and in any event not more than 28 days after the request has been received (a) where the data is kept only for purposes of direct marketing, erase the data, and (b) where the data is kept for direct marketing and other purposes, stop processing the data for direct marketing.

The data controller must notify the data subject in writing of any action taken and where appropriate, inform him of the other purposes for which the personal data is being processed. Where a data controller fails to comply with a notice the data subject may appeal to the Information and Communication Technologies Appeal Tribunal.

**ONLINE PRIVACY**

The Act does not contain specific provisions in relation to online privacy.

**KEY CONTACTS**

**BLC Robert**

**Shalinee Dreepaul Halkhoree**
Senior Associate
T +230 208 5526
shalinee.dreepaul-halkhoree@dlapiper.com

**DATA PRIVACY TOOL**

You may also be interested in our Data Privacy Scorebox to assess your organisation’s level of data protection maturity.
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’) was enacted on July 5, 2010 and entered into force on July 6, 2010.

The Executive Branch has also issued:

- 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) on December 21, 2011 (the ‘Regulations’), same which entered into force on December 22, 2011
- the Privacy Notice Guidelines on January 17, 2013 (the ‘Guidelines’) which entered into force on April 18, 2013
- the Parameters for Self Regulation regarding personal data on May 29, 2014 (the ‘Parameters’), which entered into force on May 30, 2014

The Regulations apply to all personal data processing when:

- processed in a facility of the data controller located in Mexican territory
- processed by a data processor, regardless of its location, if the processing is performed on behalf of a Mexican data controller
- where the Mexican legislation is applicable as a consequence of Mexico’s adherence to an international convention or the execution of a contract (even where the data controller is not located in Mexico), or
- where the data controller is not located in Mexican territory but uses means located in Mexico to process personal data, unless such means are used only for transit purposes.

The Law only applies to private individuals or legal entities which 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 and without the purposes of disclosure or commercial use.

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 all personal data touching on the most intimate areas of the data subject’s life, which misuse may lead to discrimination or serious risk to the data subject. In particular, the definition includes data that may reveal:

- racial or ethnic origin
- present or future health conditions
- genetic information
- religious, philosophical or moral beliefs
- union affiliation
- political views, and
- sexual orientation.

NATIONAL DATA PROTECTION AUTHORITY

The Federal Institute for Access to Information and Data Protection (Instituto Federal de Acceso a la Información y Protección de Datos) (IFAI) and the Ministry of Economy (Secretaría de Economía).

REGISTRATION

Not required.

DATA PROTECTION OFFICERS

All data controllers are required by Law to designate a personal data officer or department (jointly hereinafter referred to as the ‘Data Protection Officer’) to handle requests from data subjects exercising their rights under the Law. Data Protection Officers are also responsible for enhancing the protection of personal data within their organizations.

COLLECTION & PROCESSING

The term ‘processing’ is broadly defined to include the collection, use, communication, or storage of personal data by any means. Use includes all access, management, procurement, transfer and disposal of personal data.

In processing personal data, data controllers must observe the principles of legality, consent, notice, quality, purpose, loyalty, proportionality and accountability.

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.

Data subjects are entitled to a reasonable expectation of privacy in the processing of their personal data, – ie, reliance on the assumption that the personal data will be processed as agreed upon by the parties (in the privacy notice or otherwise) and in compliance with the Law.

To legally process personal data, data controllers must provide a privacy notice (Aviso de Privacidad) (the ‘Privacy Notice’), 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.

A comprehensive Privacy Notice must at least contain:

- the identity and domicile of the data controller collecting the data
- the purposes of the data processing
- the options and means offered by the data controller to data subjects to limit the use or disclosure of their data
- the means for exercising rights of access, correction, cancellation or objection (ARCO rights) in accordance with the provisions of the Law
- where appropriate, the types of data transfers to be made
- the procedure and means by which the data controller will notify the data subjects of changes to the Privacy Notice, and
- when processing sensitive personal data, the Privacy Notice must clearly state that sensitive personal data will be processed.

The Guidelines consider three forms of privacy notice: comprehensive, simplified and short form, depending on whether the data is personally obtained from the data subject, the data is obtained directly or indirectly from the data subject, or the space to obtain data is minimal or limited (where the space allotted for the gathering of personal data or the Privacy Notice is also minimal or limited), respectively. Each of these forms must meet specific disclosure requirements.

The data controller has the burden of proof to show that the Privacy Notice was provided to the data subject prior to the processing of his data.

Consent is required for all processing of personal data, except as otherwise provided by the Law. Implicit consent (notice and opt out) applies to the processing of personal data; express consent (notice and opt in) applies to the processing of financial or asset data; and express and written consent applies to the processing of sensitive personal data. Consent may be communicated verbally, in writing, by electronic or optical means, via any other technology, or by any other unmistakable indications. Express written consent may be obtained through the data subject’s written signature, electronic signature, or any other authentication mechanism set up for such purpose.

Consent from the data subject will not be required for the processing of personal data when:

- any law so provides
- the data is contained in publicly available sources
- the identity of the data subject has been disassociated from the data
- processing has the purpose of fulfilling obligations under 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 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**

Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it
must provide the third parties with the Privacy Notice and the purposes to which the data subject has limited the data processing. Data processing will be in accordance with what was agreed in the Privacy Notice, which shall contain a clause indicating whether or not the data subject agrees to the transfer of his data; moreover, the third party recipient will assume the same obligations as the data controller who has transferred the data.

Domestic or 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
- the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management
- the transfer is 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
- the transfer is 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
- where the transfer is necessary or legally required to safeguard public interest or for the administration of justice
- where the transfer is necessary for the recognition, exercise or defence of a right in a judicial proceeding, or
- where the transfer is 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 data processors need not to be informed nor consented to by the data subject. However, the data processor must:

- 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 confidentiality regarding the personal data subject to processing
- eliminate personal data that were processed after the legal relationship with the data controller is concluded or upon instructions of the data controller, provided there is no legal requirement for the preservation of the personal data, and
- not transfer personal data unless the data controller so determines, the communication arises from subcontracting, or if so required by a competent authority.

The agreement between the data controller and data processor related to the processing of personal data must be in accordance with the corresponding Privacy Notice provided to the data subject.

**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 unauthorised 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 establish security measures.
BREACH NOTIFICATION

Security breaches occurring at any stage of the processing which materially affect the property or moral rights of the data subject must be promptly reported by the data controller to the data subject, so that he can take appropriate action to defend his rights.

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 the latter can adopt to protect his interests
- corrective actions implemented immediately, and
- the means by which the data subject may obtain more information in regard to the data breach.

ENFORCEMENT

The Law is of public order and of general observance throughout the Mexican Republic. It has the purpose of protecting personal data held by private parties, in order to require legitimate, controlled and informed processing, and ensure privacy and the right to informational self-determination of individuals.

Data subjects can enforce their ARCO Rights, when no response is obtained from the data controller via IFAI and ultimately the court system.

IFAI may act ex officio or in response to complaints regarding violations of the Law. If any breach of the Law or its Regulations is alleged, IFAI may perform 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.

- IFAI may impose monetary sanctions that go from 100 to 320,000 times the Mexico City minimum wage (currently $70.10 Mexican pesos; however, please note that the minimum wage is updated every year). With regard to violations committed concerning the processing of sensitive personal data, sanctions may be increased up to double the above amounts.

- Three months to three years imprisonment may be imposed on any person authorised to process personal data who, for profit, causes a security breach affecting the databases under its custody. Penalties will be doubled if the sensitive personal data is involved.

- Six months to five years 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 authorised to process such data. Penalties will be doubled if sensitive personal data is involved.

ELECTRONIC MARKETING

Email marketing constitutes the processing of persona data and is subject to the provisions of the Law, among them, the obligation to provide a Privacy Notice and request consent when needed.

ONLINE PRIVACY

The Regulations and Guidelines which 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, they provide prominent notice of: the use of such technologies; the fact that personal data is being collected; and the options to disable such technologies. The notice must also specify the type of personal data being gathered and the purpose of its collection.

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**

Paola Aldrete  
Associate  
T +52 55 5261 1888  
Paola.Aldrete@dlapiper.com

**DATA PRIVACY TOOL**

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

Last modified 25 January 2018

LAW

Data protection in Monaco is regulated by Data Protection Law n° 1.165 of 23 December 1993, modified from time to time and notably by Law n° 1.353 of 4 December 2008 and for the last time by Law n° 1.454 of 30 October 2017 (DPL).

Furthermore, the Principality of Monaco is part of the Council of Europe and entered into Convention n° 108 of the European Council.

The Principality of Monaco is not part of the EU and as a consequence did not transpose Data Protection Directive 95/46/EC.

DEFINITIONS

Definition of personal data

Personal data is defined under the Data Protection Law as: ‘data enabling identification of a determined or indeterminable 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 his physical, psychological, psychological, economical, cultural, or social identity is deemed to be identifiable’.

Definition of sensitive personal data

Sensitive personal data is not expressly defined under the DPL but it is deemed 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’.

NATIONAL DATA PROTECTION AUTHORITY

The Monegasque regulator is the Commission for Control of Personal Data (Commission de Contrôle des Informations Nominatives or CCIN).

REGISTRATION

Data controllers who process personal data must inform/notify/request approval from the CCIN 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.

The notification should include the following information:

- what data is being collected

- why the data will be processed
- the categories of data subject, and
- whether the data will be transferred either within or outside the Monaco.

**DATA PROTECTION OFFICERS**

There is no requirement in Monaco for organisations to appoint a data protection officer. However, appointing a data protection officer is well perceived by the CCIN as evidence of the company’s actions to ensure compliance with the data protection legislation; however, in practice, companies in Monaco do not generally appoint data protection officers.

**COLLECTION & PROCESSING**

Data processing must be justified by:

- data subject’s consent
- a legal duty imposed to the data controller
- a public purpose
- completion of a contract entered into between the data controller and the data subject, or
- data controller’s legitimate interest, subject not to fail to respect data subject’s fundamental rights and liberties.

Where sensitive personal data is processed, one of the above conditions must be met plus one from an additional list of more stringent conditions.

The data controller must also provide the data subject with ‘fair processing information’. This includes the identity of the data controller, the purposes of processing and any other information needed under the circumstances to ensure that the processing is fair.

**TRANSFER**

As the Principality of Monaco is not part of the EU, the DPL does not distinguish between EEA jurisdictions and non EEA jurisdictions.

However, the DPL provides that the transfer of data is authorised for cross border access, storage and processing of data only to a country with equivalent protection and reciprocity.

The CCIN has established a list of the countries deemed to have an equivalent protection and reciprocity. States, and parties to Convention of the Council of Europe n° 108 relating to the protection of individuals for personal data automatic processing, are deemed to have the equivalent protection as Monaco.

Data transfers to countries with an adequate level of protection are not subject to the authorisation of the CCIN.

On the occasion of the plenary meeting on 15 April 2015, the CCIN adopted a position of principle and decided that all personal data transfers to a country or an organisation that does not ensure an adequate level of protection should, in any event, be submitted to the Commission in the form of a transfer authorisation application.

In the plenary meeting of the 16 March 2016, the CCIN affirmed that it is necessary to submit a transfer authorisation application to the Commission where personal data will be accessed from a country that does not have an adequate level of protection.

The declaration to CCIN should indicate whether it is intended for personal data to be transferred cross-border.
SECURITY

Data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data. The measures taken must ensure a level of security appropriate to the harm which might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as mentioned above, and must be appropriate to the nature of the data.

BREACH NOTIFICATION

There is no mandatory requirement in the DPL to report 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, he can serve an enforcement notice requiring the data controller to rectify the position. Failure to comply with an enforcement notice is a criminal offence and can be punished on conviction with imprisonment of 1 month to 1 year or a fine of between Eur 9,000 and Eur 90,000 or both.

ELECTRONIC MARKETING

Prior to implementing any electronic marketing activity the CCIN must be notified, as electronic marketing activities may use personal data. The law does not prohibit the use of personal data for the purpose of electronic marketing. 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.

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, and
- 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 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, or
- 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.

Persons from whom personal data is collected must be informed:

- of the identity of the data controller and, if applicable, the identity of their representative in Monaco
- of the purpose of processing
- of the obligatory or optional nature of replies
- of the consequences for them of failure to reply
- of the identity of recipients or categories of recipients
- of their right to oppose, access and rectify their data, and
- of their right to oppose the use on behalf of a third party, or the disclosure to a third party of their personal data for the purposes of prospection, particularly commercial prospection.

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 respect the provisions of the DPL.

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

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 makes use of the services of one or more service providers, they must ensure that the latter are able to comply with the obligations laid down in the two previous paragraphs.

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 organisation's level of data protection maturity.
MONTENEGRO

Last modified 24 January 2017

LAW


DEFINITIONS

Definition of personal data

The DP Law defines personal data as any information relating to an identified or identifiable natural person. The 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 his/her 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, and
- 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 seated in

Kralja Nikole 2
Podgorica
www.azlp.me

REGISTRATION

Each data controller is obliged firstly

1. to register itself as a data controller (this registration is to be performed only once), and, once the data controller’s registration is completed

2. the controller has to register separately each database containing personal data (‘Database’) which it intends to establish,
prior to the respective Database’s establishment.

Both registrations are carried out by submitting the prescribed forms which are accessible on-line and can be submitted on-line, via the DPA’s website (as identified in the section ‘National Data Protection Authority’). The type and scope of the information necessary to be submitted to the DPA when registering the Database is explicitly prescribed by the DP Law (eg, the data controller’s name and address of its registered seat, name of the Database, legal ground for the processing and processing’s purpose, types of processed data, categories of data subjects, information on the data transfer out of Montenegro (if any), etc).

Any subsequent significant change of the data processing should be registered with the DPA as well.

Exceptionally (ie if the intended data processing represents a special risk for rights and freedoms of natural persons), a data controller may, depending on the circumstances of each particular case, be obliged to obtain a prior DPA’s approval for the respective processing (eg, if biometric data is to be processed and no data subject’s consent is obtained for the respective processing).

DATA PROTECTION OFFICERS

Under the DP Law, a data controller is obliged, after the Database’s establishment, to appoint a person responsible for the protection of personal data. However, this obligation is not applicable if a data controller has less than 10 employees who process personal data.

COLLECTION & PROCESSING

A precondition for the legitimate processing of personal data is so-called informed consent of the data subject. The content of this consent is explicitly prescribed by the DP Law (for example, data subjects have to be informed on the purpose of and legal ground for the respective processing). The processing is allowed without consent only exceptionally, ie in the particular cases explicitly prescribed by the DP Law (for example, if the processing is necessary for the fulfilment of the data controller’s statutory obligations or for the protection of life and other vital interests of the data subject who cannot provide consent personally).

In any case, in order to be considered as fully compliant with the DP Law, the processing has to be done in a fair and lawful way, 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 for the processing purpose's fulfilment and the data has to be true, complete and updated.

TRANSFER

Under the transfer rules envisaged by the DP Law, personal data may be transferred to countries or provided to international organizations, where adequate level of personal data protection is ensured, on the basis of the DPA’s previously obtained consent. The DPA issues the respective consent only if it establishes that adequate measures for the protection of personal data are undertaken (the circumstances based on which the respective adequacy assessment is made include, for example, type of the data and statutory rules in force in the country to which the data is to be transferred).

However, the DPA’s consent is not required for the data transfer out of Montenegro in certain cases explicitly prescribed by the DP Law (for example, 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’s country or to any country which is on the EU list of the countries which ensure adequate level of the data protection).

SECURITY

The DP Law prescribes that both data controllers and processors are obliged to undertake technical, personnel and organizational measures for the protection of personal data from loss, destruction, unauthorized access, alteration, publication and misuse. Furthermore, the natural persons who work on data processing are obliged to keep secrecy of the processed personal data.

Additionally, data controllers are obliged to have internal rules on the personal data processing and protection (which should include the identification of the undertaken measures). The 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 provided to other users (and the conditions for the respective providing). Finally, if the processing is performed electronically, a data controller is obliged to ensure that certain information on the usage of the respective data and its users is automatically kept in the information system.

**BREACH NOTIFICATION**

There is no data security breach notification duty envisaged by the DP Law. However, the Law on Electronic Communications (‘Official Journal of Montenegro’, nos. 40/2013 and 56/2013) (‘EC Law’) does impose a duty on operators to notify, without delay, the Montenegrin Agency for Electronic Communications and Postal Activity (‘EC Agency’) and the DPA of any breach of personal data or privacy of the users. The respective users should be notified as well 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 offence liability and fines in range from EUR 6,000 to EUR 30,000 for a legal entity, and in range from EUR 300 to EUR 3,000 for a responsible person in a legal entity, plus, if some material gain was obtained by the offence’s execution, the protective measure which includes the respective gain’s seizure, may be imposed in addition to the above monetary fine.

**ENFORCEMENT**

The DPA is the authority competent 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 contravention to the DP Law
- order deletion of illegally collected data
- ban transfer of data outside of Montenegro or its providing to data users which is carried out in contravention to the DP Law, and
- 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 an offence proceeding. The offences and sanctions are explicitly prescribed by the DP Law, which includes monetary fines in range from EUR 500 to EUR 20,000 for a legal entity and in range from EUR 150 to EUR 2,000 for a responsible person in a legal entity.

Moreover, criminal liability is also a possibility since a criminal offence Unauthorized collection and usage of personal data is prescribed by the Montenegrin Criminal Code. The sanctions prescribed for this criminal offence are a monetary fine (in an amount to be determined by the court) or imprisonment up to one (1) year. 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, it is prescribed that data subjects have to be provided with a possibility to oppose the processing of their personal data for the direct marketing purposes prior to the commencement of the respective processing. Regarding the usage of sensitive personal data in direct marketing, it is explicitly prescribed that a data subject’s consent is a prerequisite for the respective processing.
Furthermore, although electronic marketing is not governed by the DP Law, there are other regulations which prescribe the rules relevant for the same 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 with prior consent of the persons to whom the respective marketing is addressed. It is absolutely forbidden to send any of the respective messages to the persons who have indicated that they do not want to receive the same (and a service provider which sends unsolicited commercial messages is obliged to establish a record of the respective persons). A violation of the respective rules is subject to offence liability and prescribed sanction is monetary fine in range from EUR 500 to EUR 17,000 (for a legal entity) and in range from EUR 100 to EUR 1,500 (for a responsible person in a legal entity). It is also prescribed that, in the case of particularly serious violations or repeated violations, a prohibition to perform business activity (lasting from three (3) months to six (6) months) may be imposed to an entity responsible for the respective violations.

ONLINE PRIVACY

There is no specific regulation explicitly governing on-line privacy (including cookies). Accordingly, the general data protection rules, as introduced by the DP Law, are, to the extent applicable, relevant for on-line privacy as well.

On the other hand, the EC Law, as defined in the section “Breach Notification” above, introduces relevant rules which are obligatory for the operators under this law. Among other, it is prescribed that a public electronic communication services’ user is particularly entitled to the protection of his/her electronic communications’ secrecy in compliance with the DP Law.

Furthermore, explicit rules on traffic data and location data are envisaged by the EC Law. Under these rules, the operators are:

1. obliged to retain certain traffic data and location data for certain purposes explicitly prescribed by the law (for example, for the detection and criminal prosecution of criminal offenders), whereas the retention period should last at least six (6) months and would not be longer than two (2) years ('Retention Obligation'), keeping in mind that this obligation does not apply to data which reveals a content of electronic communications

2. regarding traffic data related to subscribers/users which is not subject to the Retention Obligation, an operator is obliged 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

   1. if 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

   2. if 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 moment), and

3. regarding location data which is not subject to the Retention Obligation, an operator is allowed to process it but only with a data subject’s consent (which can be withdrawn at any moment) or without the same if the respective data is modified in a way that it cannot be linked to a particular person.

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/

Milena Ronevi
Associate
T office +382 20 238 991
milena.roncevic@karanovic-nikolic.com

Sanja Spasenovic
Attorney at law in cooperation with Karanovi & Nikoli
T Office +381 11 3094 200/ Direct T +381 11 3955 413
Sanja.Spasenovic@karanovic-nikolic.com

DATA PRIVACY TOOL

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

Last modified 26 January 2017

LAW

Law No 09-08 dated on 18 February 2009 relating to protection of individuals with regard to the processing of personal data and its implementation Decree n° 2-09-165 of 21 May 2009 ("Law").

DEFINITIONS

Definition of personal data

Pursuant to article 1 of the Law, the personal data is defined as any information regardless of their nature, and format, relating to identified or identifiable person.

Definition of sensitive personal data

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 Law).

NATIONAL DATA PROTECTION AUTHORITY


REGISTRATION

The processing of Personal Data is subject:

- to a prior authorization from the Data Protection National Commission (Commission Nationale de Protection des Données Personnelles) when the processing concerns:
  a. sensitive data (e.g. revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, including genetic data)
  b. using personal data for purposes other than those for which they were collected
  c. genetic data, except for those used by health personnel and that respond to medical purposes
  d. data relating to offenses, convictions or security measures, except for those used by the officers of the court, and
  e. data which includes the number of the national identity card of the concerned person, or

- to a prior declaration to be filed with the Personal Data Protection Commission.
The declaration and authorization includes a commitment that the personal data will be treated in accordance with the Law.

The prior declaration and authorization shall include, but is not limited to, 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 processing envisaged
- 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 envisaged 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 by law, and the measures taken to facilitate the exercise of these rights
- a general description allowing a preliminary assessment of the appropriateness of the measures taken to ensure the confidentiality and security of processing, 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

N/A

COLLECTION & PROCESSING

The personal data must be:

- treated fairly and lawfully;
- collected for specific, explicit and legitimate purposes;
- adequate, relevant and not excessive;
- accurate and necessary and kept up-to-date; and
- 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 concerned person.

However, the processing of personal data can be performed without the approval of the concerned person provided that the information relates to the:

- compliance with a legal obligation to which the concerned person or the person in charge of the processing are submitted
- 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
- protection of the vital interests of the concerned person, 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
- fulfilment of the legitimate interests pursued by the person in charge of the processing or by the recipient, subject not to disregard the interests or fundamental rights and freedoms of the concerned person.

TRANSFER

The personal data must be subject to prior authorization from the National Commission before any transfer to a foreign state.

Furthermore, 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.

However, the data processor can transfer personal data to any foreign state which does not satisfy the conditions.
mentioned above (i.e. ensure an adequate level of protection of privacy and fundamental rights and freedoms of individuals), if the person to whom the data relates has expressly consented to the transfer.

**SECURITY**

Article 23 of the Law provides that the data processor 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 against any form of illicit processing.

In addition, the data processor who carries out processing on his own behalf must choose a subcontractor that 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**

N/A

**ENFORCEMENT**

The Data Protection National Commission ensures compliance with the provisions of the Law.

Article 50 to 64 provides that non-compliance with the provisions of the Law is punishable by a fine ranging from MAD 10,000 to MAD 600,000 and/or imprisonment between three months and four years.

When 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 offence, and
- the closure of the establishment(s) of the legal person where the offense was committed.

**ELECTRONIC MARKETING**

Direct prospecting by means of an automated calling machine, a fax machine, e-mails 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 prospecting via e-mails may be authorized if the recipient details have been received directly from him.

Unwanted emails can only be sent without consent in the following cases:

- the contact details were provided in the course of a sale
- the marketing relates to a similar product, and
- the recipient was given a method to opt-out of the use of their contact details for marketing when they were collected.

**ONLINE PRIVACY**

General Data Protection principles apply.
KEY CONTACTS

Christophe Bachelet
Partner
T +33 1 40 152 559
Christophe.Bachelet@dlapiper.com

Mehdi Kettani
Partner
Mehdi.Kettani@dlapiper.com

Kawtar Bedraoui Idrissi
Associate
T +212(0)520 42 78 33
kawtar.bedraoui@dlapiper.com

DATA PRIVACY TOOL

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

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 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.

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.

**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 .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.

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.

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, a change which is currently forecast for Spring 2019. 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 partially regulated in Article 11.7 of the Dutch Telecommunications Act (Tw). In the context of this Article electronic marketing could be defined as SMS, e-mail, fax and similar media for the purposes of unsolicited communication related to commercial, charitable or ideal purposes without the individuals’ prior express consent.

Electronic marketing directed to corporations does not require prior consent if:

- the advertiser/electronic marketer uses electronic address data which are meant to be for this particular purpose, and
- if the individual is located outside the EU, the advertiser/electronic marketer complies with the relevant rules of that particular country in this respect.

On the basis of Article 11.7 of the Tw electronic marketing to individuals is in principle prohibited. If certain conditions are being met, such as prior express consent, electronic marketing directly to individuals can be allowed. Furthermore, electronic marketing to individuals is also allowed if it is restricted to the marketing of existing customers and restricted to similar products/services of the advertiser/electronic marketer. In the latter case, the advertiser/electronic marketer is obliged to provide opt-out possibilities to his customers when obtaining the data from the customers and in every marketing message sent.

**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 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 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 these data are being processed in anonymous form
• with informed consent of the individual

Cookie Compliance

The Netherlands implemented the E-Privacy Directive through the Dutch Telecommunications Act in Article 11.7a (hereinafter: Article 11.7a). The Authority for Consumers and Markets (“ACM”) is entrusted with the enforcement of Article 11.7a.

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). Implicit consent is accepted under Dutch law. Please note that the website operator is 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 that have little or no impact on the user’s privacy (e.g. first party cookies).

The use of analytic cookies, affiliate or performance cookies used for the purpose of paying affiliates or cookies used for testing the effectiveness of certain banners will be allowed without consent, on the condition that:

• the data collected by such cookies are not used for, among other things, creating profiles by the website owner and/or the third party with whom the data are shared; and
• website owners sharing the data with a third party take additional measures in order to limit any possible privacy impact.

The information collected through cookies are to be considered “personal data”, unless the party which places the cookies can prove otherwise. This goes only for tracking cookies, whereby the surfing behaviour of customers on several different websites is being observed (and the information obtained is being used for commercial purposes).

In case of violation of electronic marketing or online privacy legislation, the ACM can impose fines of up to EUR 900,000 per violation.

KEY CONTACTS

Richard van Schaik
Partner & Co-Chair of EMEA Data Protection and Privacy Group
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 organisation’s level of data protection maturity.
NEW ZEALAND

LAW

The Privacy Act 1993 (‘Act’) governs 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. Codes currently in place are:

- Credit Reporting Privacy Code
- Health Information Privacy Code
- Justice Sector Unique Identifier Code
- Superannuation Schemes Unique Identifier Code
- Telecommunications Information Privacy Code

Enforcement is through the Privacy Commissioner.

DEFINITIONS

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.

Definition of personal data

Personal data is ‘personal information’ under the Act and 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

Although no differentiation is made between how different types of personal information are to be treated under the Act, 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.
REGISTRATION

There is no obligation on agencies to notify the Privacy Commissioner that they are processing personal information. However, the Privacy Commissioner may require an agency to supply information for the purpose of publishing or supplementing a directory or to enable the Privacy Commissioner to respond to public enquiries in this regard.

The Privacy Commissioner may from time to time publish a directory of personal information including:

- the nature of any personal information held by an agency
- the purpose for which personal information is held by an agency
- the classes of individuals about whom personal information is held by an agency
- the period for which personal information is held by an agency
- the individuals entitled to access personal information held by an agency and the conditions relating to such access, and
- steps to be taken by an individual wishing to obtain access to personal information held by an agency.

DATA PROTECTION OFFICERS

The Act requires each agency to appoint within that agency, one or more individuals to be a privacy officer. The privacy officer’s responsibilities include:

- the encouragement of compliance with the personal information privacy principles 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.

Provided the person appointed a privacy officer is within the agency, that person does not have to be a New Zealand citizen or reside in New Zealand.

Failure to appoint a privacy officer or obstructing or hindering the Privacy Commissioner is an offence under the Act. The maximum penalty on conviction is a fine of $2,000.

COLLECTION & PROCESSING

Subject to specific exceptions, agencies may collect, store and process personal information in accordance with the following 12 information privacy principles:
1. The personal information is needed for a lawful purpose connected with the agency’s work.

2. The personal information is collected directly from the relevant person.

3. Before the personal information is collected, the agency has taken reasonable steps to ensure that the person knows that the information is being collected; the purpose for which it is being collected; the intended recipients; the name and address of the agency collecting and holding the information; if the information is authorised or required by law, the applicable law and the consequences if the requested information is not provided; and that the person concerned may access and correct the information.

4. The personal information is not collected in an unlawful or unfair way or in a way that unreasonably invades a person’s privacy.

5. The personal information must be kept reasonably safe from being lost, accessed, used, modified or disclosed to unauthorised persons.

6. If the personal information is readily retrievable, the relevant person is entitled to know whether information is held and to have access to it.

7. The relevant person is entitled to request correction of the personal information. If the agency will not correct the information, the person may provide a statement of the correction sought to be attached to the personal information.

8. Before it is used, the agency must ensure that the personal information is accurate, up to date, complete, relevant and not misleading.

9. The personal information may not be kept for any longer than it is needed.

10. Subject to certain exceptions, personal information collected for one purpose may not be used for another purpose.

11. An agency must not disclose personal information to another person, body or agency except in specific circumstances.

12. An agency may only assign a unique identifier to an individual if it is needed for the agency to carry on its work efficiently and may not assign a unique identifier to an individual if the same identifier is used by another agency.

Personal information does not need to be collected directly from the relevant person if:

- the personal information is publicly available
- the relevant person authorises collection of the personal information from someone else
- non-compliance would not prejudice the interests of the relevant individual
- the personal information is being collected for a criminal investigation, enforcement of a financial penalty, protection of public revenue or the conduct of court proceedings
- compliance would prejudice the purpose of the collection of the personal information or is not practical in the circumstances, and
- the personal information will be used in a way which will not identify the person concerned.

**TRANSFER**

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.

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 OECD Guidelines, which include:

- the collection limitation principle (there should be limits to the collection of personal data)
- the data quality principle (personal data should be accurate, complete and kept up to date)
- the purpose specification principle (the purposes for which personal data are collected should be specified)
- the use limitation principle (personal data should not be used otherwise than in accordance with the purpose specification principle, except with the consent of the data subject or by authority of law)
- the security safeguards principle (personal data should be protected by reasonable security safeguards)
- the openness principle (there should be a general policy of openness about developments, practices and policies relating to personal data)
- the individual participation principle (individuals should have the right to obtain confirmation of whether a data controller holds their personal data, to have that data communicated to him/her, to be given reasons if a request for that data is denied and to be able to challenge that denial, and to challenge data relating to him/her and have that data erased, rectified, completed or amended if successful), and
- the accountability principle (a data controller should be accountable for complying with the above principles).

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 19 December 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 recent decision in the Schrems case, where the European Commission’s decision to recognise the safe harbour agreement with the USA was invalidated, there have been calls to review New Zealand’s adequacy status, primarily due to New Zealand’s membership with the Five Eyes network. The USA safe harbour arrangement was one of six adequacy decisions issued by the Commission for countries outside the European Union of which another of those applies to New Zealand. However, to date this has not been acted upon by the European Commission.

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, except with the authority of the agency, and
other misuse or unauthorised disclosure.

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**

There is no mandatory requirement in the Act to report an interference with privacy.

Any person may make a complaint to the Privacy Commissioner alleging an action is, or appears to be, an interference with the privacy of an individual. For there to be an interference with privacy, there must be a breach of the law and the breach must lead to financial loss or other injury, an adverse effect on a person’s right, benefit, privilege, obligation or interest or significant humiliation, loss of dignity or injury to a person’s feelings. There is no requirement to show harm in a complaint about access to, or correction of, personal information. An unauthorised disclosure of personal information is sufficient to breach the Act.

**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. The Privacy Commissioner is not able to issue a formal ruling or determination and cannot begin prosecution proceedings or impose a fine.

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.

**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 includes email, fax, instant messaging, mobile/smart phone text (TXT) and image-based messages of a commercial nature – but does not cover internet pop-ups or voice telemarketing) with a New Zealand link (messages sent to, from or within New Zealand)
- 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
Data Protection Laws of the World

New Zealand

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/

John Hannan  
Partner  
T +64 9 300 3843  
john.hannan@dlapiper.com

**DATA PRIVACY TOOL**

You may also be interested in our Data Privacy Scorebox to assess your organisation’s level of data protection maturity.
Nigeria does not have a comprehensive legislative framework on the protection of personal data. However, there are a few industry-specific and targeted laws and regulations that provide some privacy-related protections, which include:

- The Constitution of the Federal Republic of Nigeria, 1999 (As Amended) (‘the Constitution’) which provides for the fundamental rights of its citizens and upholds the right of privacy as sacrosanct. Section 37 thereof provides for the guarantee and protection of the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications.

- The Freedom of Information Act, 2011 (‘FOI Act’) which 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. Also, 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).

- The Child Rights Act No. 26 of 2003 (the ‘Child Rights Act’) regulates the protection of children (persons under the age of 18 years). This Act limits access to information relating to children in certain circumstances.

- The Consumer Code of Practice Regulations 2007 (‘the NCC Regulations’) issued by the regulator of the telecommunications industry in Nigeria, the Nigerian Communications Commission (‘NCC’). The NCC Regulations provide that all licensees must take reasonable steps to protect customer information against improper or accidental disclosure, and must ensure that such information is securely stored and not kept longer than necessary. It also provides that 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.

- In 2011, the NCC issued the Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011. Section 9 of the Regulation provides that subscribers information contained in the Central Database shall be held in strict confidentiality basis and no person or entity shall be allowed access to any subscriber’s information that is on the Central Database except as prescribed by the Regulation. “Central Database” is defined in the Regulation to mean subscriber information database, containing the biometric and other registration information of all Subscribers. Section 21 of the Regulation provides penal sanctions for violators.

- The National Information Technology Development Agency (‘NITDA’) which is the national authority responsible for planning, developing and promoting the use of information technology in Nigeria, and which issues the Guidelines on Data Protection (‘NITDA Guidelines’) pursuant to the NITDA Act 2007. The NITDA Guidelines prescribe guidelines for organisations that obtain and process personal of Nigeria residents and citizens within and outside Nigeria for protecting such personal data. The NITDA Guidelines apply to federal, state and local government agencies and institutions as well as private sector organisations that own, use or deploy information systems within the Federal Republic of Nigeria.
The Cybercrimes (Prohibition, Prevention Etc) Act 2015 provides a legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. The Act provides for the retention and protection of Data by financial institutions, criminalizes the interception of electronic communications etc.

The National Identity Management Commission (NIMC) is the body empowered to establish, operate and manage the National Identity Management System (NIMS), carry out the enrolment of citizens and legal residents as provided for in the Act, create and operate a National Identity Database, issue 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 contained in the Database with respect to a registered individual entry without the authorization of the Commission. The Commission is however empowered to provide another person with information recorded in the individual's entry in the Database without the individual's consent. In this instance, the provision of such information is in the interest of National Security, necessary for purposes connected with the prevention or detection of crime or for any other purpose specified by the Commission in a regulation.

The Immigration Service is basically the body responsible for the modalities required for the entry and exit of persons within and outside Nigeria. The Immigration Act does not specifically provide for issues relating to data protection and privacy however its Privacy Policy deals with various subjects including Information sharing. The Policy states that personal information will not be used for commercial purposes or shared with individuals outside the Nigeria Immigration Services. However, personal information may be shared to prevent or detect fraud or technical issues; consent is obtained; there is a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against imminent harm to the rights, property or safety of Google, its users or the public as required or permitted by law; a payment instrument has been used for payment and must be disclosed in order to process payment, such information must be given to the Immigration Service subsidiaries and affiliated companies for the purpose of processing personal information on behalf of the Immigration Service.

DEFINITIONS

Definition of personal data

The NITDA Guidelines define personal data as any information relating to an identified or identifiable natural person (‘data subject’): information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address.

The Registration of Telephone Subscribers Regulation 2011 provides that personal information refers to:

- the full names (including mother’s maiden name)
- gender
- date of birth
- residential address
- nationality
- state of origin
- occupation and such other personal information
- contact details of subscribers, as specified in the Registration Specifications.

Definition of sensitive personal data

The NITDA Guidelines define personal sensitive data as data relating to:

- religious or other beliefs
- sexual orientation
- health
- race
- ethnicity
• political views
• trade union membership
• criminal record.

**NATIONAL DATA PROTECTION AUTHORITY**

There is no specific authority bestowed with the responsibility of the protection of data, however sector specific regulatory agencies including NITDA, NCC etc provide services relating to the protection of data.

**REGISTRATION**

There is no requirement to register databases.

**DATA PROTECTION OFFICERS**

The NITDA Guidelines provide that organisations should designate an employee as the Data Security Officer of that organisation whose duties shall include:

• Ensuring that the organization adheres to the stated policies
• Ensuring continued adherence to data protection and privacy policies and procedures
• Ensuring that individual data is protected
• Providing for effective oversight of the collection and use of individual information
• Being responsible for effective data protection and management within that organization; and ensuring compliance with the privacy and data security policies
• Training and education for employees to promote awareness of and compliance with the privacy and data security policies
• Developing recommended practices and procedures to ensure compliance with the privacy and data security policies.

**COLLECTION & PROCESSING**

The collection and processing of personal data has to be done pursuant to the data subject’s consent or as specifically provided by law. The NITDA Guidelines establish the scope of permitted collection and processing of personal data.

**Collection**

1. Personal data should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

2. Collection of personal data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs, trade-union membership, health or sex life can only be undertaken where:

• the data subject has given unambiguous consent
• the collection and processing is necessary for carrying out the obligations and specific function of the data controller in the field of employment
• the collection and processing is necessary to protect the interest of the data subject or another person where the data subject is incapable of giving consent
• the collection and processing relates to data which are manifestly made public by the data subject
the collection and processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body and on the condition that the processing relates solely to its members or persons who have regular contact with it in connection with its purposes

the collection and processing is necessary for the establishment, exercise or defence of legal claims.

3. Where data was not obtained from the data subject, the controller or third party should at the time of recording the personal data or if a disclosure to a third party is envisaged, provide the data subject no later than when the data are first disclosed with the following information (except where the data object already has it):

- the identity of the controller and of the representative (if any)
- the purposes of the processing
- any further information such as:
  - the categories of data concerned
  - the recipients or categories of recipients
  - the existence of the mechanism for access to and the mechanism to rectify the data concerning the data subject.

**Processing**

1. Personal data may be processed only if the data subject has given unambiguous consent and 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
- necessary for compliance with a legal obligation to which the controller is subject
- necessary to protect the interest of the data subject
- 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 third party to whom the data are disclosed
- required for the purposes of management of health-care services subject to professional secrecy
- related to offences or criminal convictions
- necessary for legitimate interests pursued by the data controller or third party or parties to whom the data are disclosed, save where such interests are overridden by the interests or privacy of the data subject.

2. A complete register of criminal convictions is to be kept only under the control of official authority. Data relating to administrative sanctions or judgments in civil cases are to be processed under the control of official authority.

3. Every data subject shall be able to obtain from the controller without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to data subject are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed
- communication to the data subject in an intelligible form of the data undergoing processing and of any available information as to their source
knowledge of the logic involved in any automatic processing of data concerning data subject at least in the case of the automated decisions

- rectification, erasure or blocking of data which does not comply with the provisions of the NITDA guidelines, in particular because of the incomplete or inaccurate nature of the data

- notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with these guidelines.

TRANSFER

The NCC Regulations provide that 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.

The NITDA Guidelines provide that personal data must not be transferred outside Nigeria unless adequate provisions are in place for its protection and where the controller finds that any country does not ensure an adequate level of protection of such personal data within the requirements of the Guidelines, the controller must prevent any transfer of data to the country in question. It further states that the following must be considered if a requirement exists to send or transfer data outside Nigeria:

- if the receiving country has adequate data protection legislation equivalent to that of Nigeria
- if it is necessary to send the data as part of the fulfilment of a contract
- if the data subject has consented
- if the data is being processed outside Nigeria by another office of the same firm which is established within Nigeria
- if there is a contract in place between the data controller and the receiving organisation which provides for the adequate protection of personal data.

The RTS Regulations make it mandatory for subscriber’s information not to be transferred outside Nigeria.

SECURITY

To ensure the security of the data, the NITDA Guidelines provide that the data controller should implement technical and organizational measures to secure 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.

BREACH NOTIFICATION

As far as we know, there is no mandatory legal requirement to report data security breaches or losses to the authorities or to data subjects.

Mandatory breach notification

Comments are the same as above.

ENFORCEMENT

Under the NCC Regulations, any licensee that contravenes any of the provisions of the Regulations would be in breach and would be liable to such fines, sanctions or penalties as may be determined by the Commission from time to time.

A breach of the NITDA Guidelines which was made pursuant to the NITDA Act 2007 would be considered a breach of the NITDA Act.
ELECTRONIC MARKETING

The NCC Regulations on Consumer Code of Practice 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
- that 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 also 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.

The NCC Legal Guidelines for Internet Service Providers (ISP) provide 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 request 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.

The Nigerian Code of Advertising Practice Sales Promotion and other Rights/Restrictions on Practice provides that:

- All advertising and marketing communications directed to the Nigerian market using internet and other electronic media are subject to the laws regulating advertising practice in Nigeria.
- Without prejudice to any other restrictions or obligations imposed by the Act or under the code on advertising, all advertisements directed towards the Nigerian market using the Internet or any other electronic media must comply with the following requirements:
  - The commercial nature of the communication must not be concealed or misleading, it should be made clear in the subject header.
  - There should be clarity of the terms of the offer and devices should not be used to conceal or obscure any material factor such as: the price or other sale conditions likely to influence the customers’ decision.
  - There should be clarity as to the procedure for concluding a contract.
  - Due recognition must be given to the standards of acceptable commercial behavior held by public groups before
the posting of marketing communications to such groups using electronic media.

- Unsolicited messages should not be sent except where there are reasonable grounds to believe that the consumers who received such communications will be interested in the subject matter or offer.

- All marketing communications sent via electronic media should include a clear and transparent mechanism enabling the consumer to express the wish not to receive future solicitations.

In addition to respecting the consumer’s preferences, expressed either directly to the sender or through participation in a preference service programme, care should be taken to ensure that neither the marketing communication itself, nor any application used to enable consumers to open other marketing or advertising messages, interferes with the consumer’s normal usage of electronic media.

**ONLINE PRIVACY**

The established rights of privacy (as guaranteed by the Constitution) apply equally to electronic media, such as mobile devices and the Internet. So, violations of these rights may be subject to civil enforcement. Furthermore the Cybercrimes (Prohibition, Prevention Etc) Act promotes cybersecurity, protects electronic communications and privacy rights.

**KEY CONTACTS**

Jackson, Etti & Edu  
www.jacksonettiedu.com

Uwa Ohiku  
Managing Partner  
T (234) 01 461 7379 (234) 01 462 6842  
uwaohiku@jacksonettiedu.com

**DATA PRIVACY TOOL**

You may also be interested in our Data Privacy Scorebox to assess your organisation's level of data protection maturity.
DATA PROTECTION LAWS OF THE WORLD

NORWAY

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 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.

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.

**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 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.

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, a change which is currently forecast for Spring 2019. 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 (e.g., an email address is likely to be ‘personal data’ for the purposes of the Act).

Pursuant to the Marketing Control Act (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, Nw: Ehandelsloven, section 9).

**ONLINE PRIVACY**

**Traffic Data**

Traffic data is defined in Norwegian Regulation relating to Electronic Communications Networks and Electronic Communications Services (Nw: Ekomforskriften F16.02.2004 nr 401) 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 anonymised when it is no longer necessary for the purpose of the transmission of a communication (Electronic Communications Act 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 user’s consent to processing may be expressed by using the appropriate settings of a browser or other application. Where the use of a cookie involves processing of personal data, the service providers will have to comply with the additional requirements of the Data Protection Act.

---

**KEY CONTACTS**

Petter Bjerke  
Partner  
T +47 2413 1654  
petter.bjerke@dlapiper.com

Jan Sandtrø  
Partner  
T +47 2413 1614  
jan.sandtro@dlapiper.com

---

**DATA PRIVACY TOOL**

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

LAW

There is, at the date of publication, no legislation regulating the protection of data in Pakistan.

DEFINITIONS

Definition of personal data

In the absence of any legislation regulating the protection of data in Pakistan, the term ‘personal data’ is undefined.

Definition of sensitive personal data

In the absence of any legislation regulating the protection of data in Pakistan, the term ‘sensitive personal data’ is undefined.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in Pakistan.

REGISTRATION

Data controllers or collectors do not need to register with any authority.

DATA PROTECTION OFFICERS

Organisations in Pakistan are not required to appoint a data protection officer.

COLLECTION & PROCESSING

Data controllers can collect and process personal data under any conditions.

TRANSFER

Although the transfer of data to third parties is not specifically regulated under the laws of Pakistan, data cannot be transferred from Pakistan to a country which is not recognised by Pakistan. Pakistan currently does not recognise 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. Furthermore, data can only be transferred to India if such a transfer can be justified by the transferor.

Besides being regulated by contractual terms, data collated by, inter alia, banks, insurance firms, hospitals, defence establishments and other ‘sensitive’ installations/institutions cannot be transferred to any individual/body unless it is transferred with the
permission of the relevant regulator or similar bodies on a confidential basis. Additionally, in certain cases data cannot be transferred without the permission of the relevant client/customer.

Please note however that in the case of banks/financial institutions, the secrecy of banking transactions must be maintained.

SECURITY

Data controllers do not have to fulfil any security requirements.

BREACH NOTIFICATION

Data security breaches or losses do not have to be reported or notified to any body or individual.

ENFORCEMENT

In the absence of any legislation in the sphere of data protection no body or entity enforces any law. Enforcement and appropriate relief may however be sought through courts of law having jurisdiction in the matter.

ELECTRONIC MARKETING

There is, at the date of publication, no subsisting legislation regulating electronic marketing in Pakistan. Please note that an earlier law promulgated in this regard has since lapsed.

ONLINE PRIVACY

The Prevention of Electronic Crimes Act, 2016 has criminalized, amongst other things: unauthorized access to information systems or data; the unauthorized copying or transmission of data; the unauthorized use of identity information; and "offences against the dignity of a natural person", which includes transmitting information through an information system which "harms the reputation or privacy of a natural person". However, there is no law specifically regulating the manner in which an individual’s private information may be stored or transmitted online.

KEY CONTACTS

LMA Ebrahim Hosain
www.lma-eh.com

Darakhshan Sheikh Vohra
Partner
LMA Ebrahim Hosain
T +9221 3583 5101 – 104
d.vohra@lma-eh.com

Ali Qaisar
Associate
LMA Ebrahim Hosain
T +9221 3583 5101-104
a.qaisar@lma-eh.com

DATA PRIVACY TOOL

http://www.dlapiperdataprotection.com
You may also be interested in our Data Privacy Scorebox to assess your organisation’s level of data protection maturity.
PANAMA

LAW

In recent years, Panama has taken significant legislative steps to regulate electronic data protection and internet commerce. However, this regime remains a work in progress.

The primary laws and regulations thus far enacted are Law 51 of 22 July 2008, as amended by Law 82 of 9 November 2012 (‘Law 51’), and Executive Decree No. 40 of 19 May 2009 (‘Decree 40’). The central purpose of both Law 51 and Decree 40 is to regulate the creation, utilization and storage of electronic documents and signatures in Panama, through a registration process and the supervision of providers of data storage services. Law 51 and Decree 40 provide for enforcement through the General Directorate of Electronic Commerce (Dirección General de Comercio Electrónico) (‘DGCE’).

DEFINITIONS

Definition of personal data

Personal Data is not expressly defined under Panamanian law. However, it is generally deemed to include information that can specifically identify an individual, such as one’s name, postal address (including billing and shipping addresses), telephone number, e-mail address, credit card number, or a username.

Definition of sensitive personal data

‘Sensitive Personal Data’ is not defined under Panamanian Law.

NATIONAL DATA PROTECTION AUTHORITY

The General Directorate of Electronic Commerce (Dirección General de Comercio Electrónico)

Plaza Edison, Sector El Paical, Floors 2 & 3.

T (507) 560-0600
(507) 560-0700
F (507) 261-1942

contactenos@mici.gob.pa

REGISTRATION

Under Decree 40, electronic data storage companies and companies engaged in online electronic signature verification must register with the DGCE. For companies otherwise engaged in e-commerce-related activities, registration with the DGCE is
voluntary and can be completed online and free of cost. Registration must occur no later than 15 days prior to the commencement of data processing activities and shall include, *inter alia*, the following information:

- name of the company
- company’s physical address, telephone and fax number
- legal representative of the company
- company’s internet address or URL
- contact email provided by company to customers
- public Registry and Ministry of Commerce Registration Information
- in the event that an undertaken activity requires specific authorization or permits, evidence thereof
- tax Identification Number
- description of services offered by the company, including pricing information and applicable taxes, and
- the Company’s code of conduct.

Law 51 and Decree 40 set forth certain additional registration requirements for companies that are engaged in each of the activities for which registration is mandatory.

Further, pursuant to recently enacted regulations, individuals or entities who wish to electronically interact with government entities must first register by activating a user account and executing a release form that is available both physically and online. To the extent necessary, government entities may also request a petitioner’s consent to access such petitioner’s personal information that is available on a different government entity’s system.

**DATA PROTECTION OFFICERS**

Appointment of a data protection officer is not required.

**COLLECTION & PROCESSING**

In Panama, personal information is protected at the constitutional level. The Constitution provides that any person or entity that obtains personal information and/or personal documents, either from a person or a company who provides such information willingly, or through any other means, may not disclose such information without the consent of its lawful owner (there is no specific definition or explanation of who is considered the ‘lawful owner’ of personal information). An exception to the consent rule is the disclosure of such information pursuant to a valid judicial or governmental request.

The disclosure of personal information without consent is also prohibited by the Panamanian Criminal Code. Criminal penalties apply to the disclosure of personal information when the disclosure causes harm to the information’s lawful owner. Law 51 specifically establishes that this criminal law prohibition applies to electronically stored information.

Panamanian law further requires that providers of online data storage services take reasonable measures to ensure that company personnel who come into contact with confidential information do not have a criminal record, have obtained the necessary technical skills to handle such data and information, and possess reasonable knowledge of existing legal restrictions related to the disclosure of such information. Although this prohibition is specifically intended to apply to entities that provide online data storage services, it is not unforeseeable that it could also be construed to apply to any company engaged in e-commerce.

**TRANSFER**
Despite the Panamanian e-commerce regulatory framework not being fully developed, existing regulations follow the constitutional principle that the consent of the lawful owner is required for the transfer of any personal information.

Pursuant to Law 51, when a customer provides his email address during the process of acquiring or subscribing to a service offered online, the company providing such service must disclose to the customer its intent to use the email address in the future for commercial communications and, further, must obtain the customer’s express consent for such purposes.

The client or customer must also be able to revoke such consent easily, through a simple process made available by the provider of the service.

While the manner in which this restriction appears to have been drafted suggests that it applies exclusively to online service providers, its broader application to all companies that sell products online or are engaged in e-commerce activities is foreseeable.

**SECURITY**

Decree 40 establishes certain security requirements applicable only to electronic data storage and electronic signature verification companies, for whom registration with the DGCE is mandatory. The main requirements are adherence to the security parameters periodically published by the DGCE, and the performance of annual self-audits, the results of which must be filed with the DGCE in order for the company to renew its registration. In addition, these companies must create a disaster recovery plan that allows such providers to re-establish regular operations within twelve hours of the occurrence of a disruptive event.

No similar provisions have been enacted with respect to companies who engage in other types of e-commerce, ie, those for whom registration is voluntary.

**BREACH NOTIFICATION**

Law 51 does not require breach notification.

**ENFORCEMENT**

The DGCE is responsible for enforcement of the existing e-commerce and related regulations, including the publication of additional complementary regulations. Sanctions include the suspension or permanent ban of the activities of companies that infringe certain regulations, as well as fines of up to US$150,000.

**ELECTRONIC MARKETING**

With respect to email advertising, Panamanian law requires that all such emails:

- state that they are commercial communications
- include the name of the sender, and
- 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 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/

Diego Herrera
T +507 303 0303
dherrera@gala.com.pa

James Sattin
T +507 303 0303
jsattin@gala.com.pa

Jose Luis Sosa
T +507 303 0303
jsosa@gala.com.pa

DATA PRIVACY TOOL

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

LAW

The Philippines recently enacted the Data Privacy Act of 2012 (the ‘Act’) or Republic Act No. 10173, which took effect on 8 September 2012.

DEFINITIONS

Definition of personal data

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

- 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 Philippines 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 data**

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, licences 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 Act provides for the creation of a National Privacy Commission. As of 21 January 2015, the National Privacy Commission has not been constituted.

**REGISTRATION**

There is no system of mandatory registration provided in the Act.

**DATA PROTECTION OFFICERS**

The Personal Information Controller of an organisation must appoint a person or persons who shall be accountable for the organisation’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 Act does not specifically provide for the citizenship and residency of the data protection officer. The Act likewise does not specifically provide for penalties relating to the incorrect appointment of data protection officers.

**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 defence 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 authorising 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 personal information controller 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 personal information controller 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 organisations and their associations, provided:
  ○ such processing is only confined and related to the bona fide members of these organisations 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

The transfer of Personal Information is permitted without any restrictions or prerequisites, but the Personal Information Controller remains 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. The transfer, however, of sensitive personal information to third parties is prohibited.

SECURITY

The personal information controller must implement reasonable and appropriate organisational, 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 organisation 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 National Privacy Commission may issue:

• safeguards to protect its computer network against accidental, unlawful or unauthorised 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 personal information controller 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 personal information controller who are involved in the processing of such personal information.

BREACH NOTIFICATION

The Personal Information Controller is required to promptly notify the National Privacy Commission and the affected data subjects when it has reasonable belief that sensitive personal information or other information has been acquired by an unauthorised person, and that:

• such personal information may, under the circumstances, be used to enable identity fraud, and

• the Personal Information Controller or the National Privacy Commission believes that such unauthorised 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.

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 National Privacy Commission may also authorise postponement of notification where such notification may hinder the progress of a criminal investigation related to a serious breach.

Notification is not required if the National Privacy Commission determines:

- that notification is unwarranted after taking into account compliance by the Personal Information Controller with the Act and the existence of good faith in the acquisition of personal information, or
- in the reasonable judgment of the National Privacy Commission, such notification would not be in the public interest or in the interests of the affected data subjects.

**ENFORCEMENT**

The National Privacy Commission is responsible for ensuring compliance of the Personal Information Controller 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, publicise any such report. Additionally, the National Privacy Commission 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 National Privacy Commission, 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 authorised by the Act or any existing law, or
  - for purposes not authorised by the data subject or otherwise authorised under the Act or under existing laws

- providing access to personal information or sensitive personal information due to negligence and without being authorised 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 National Privacy Commission pursuant to Section 20(f) of the Act

- disclosing by any personal information controller or personal information processor 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

- [http://www.dlapiperdataprotection.com](http://www.dlapiperdataprotection.com)
disclosing, with malice or in bad faith, by any personal information controller or personal information processor or any of its officials, employees or agents of unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her.

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

Section 4(c)(3) of the CPA was struck down by the Supreme Court for violating the constitutionally guaranteed freedom of expression.

ONLINE PRIVACY

The CPA is the first law in the Philippines which specifically criminalises 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 penalises acts that violate an individual’s rights to online privacy, particularly those interferences against the confidentiality, integrity and availability of computer data and systems.

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 penalised 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 or the regulation of the use of Cookies.

**KEY CONTACTS**

Romulo Mabanta Buenaventura Sayoc & De Los Angeles  
www.romulo.com/

**Eileen Rosario Cordero-Batac**  
Partner  
T +63 2 555 9555  
eileen.batac@romulo.com

**Catherine O. King Kay**  
Associate  
T +63 2 555 9555  
catherine.kingkay@romulo.com

**DATA PRIVACY TOOL**

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

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.

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 referred to as the 'previous PDPA'). A number of provisions of the Telecommunications Act of 16 July 2004 (consolidated text: Journal of Laws 2017, item 1907, hereinafter referred to as 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 others, employment and banking matters also contain specific regulations on the processing of personal data.

In relation to the GDPR, on 12 September 2017, two draft acts on personal data protection law were published in Poland. The first one was the draft of the PDPA which came into force on 25 May 2018 (Personal Data Protection Act of 10 May 2018 (Journal of Laws of 2018, item 1000, hereinafter referred to as the ‘new PDPA’), while the second is the draft act on the provisions implementing the new PDPA (it contains a number of amendments of sectorial regulations (hereinafter referred to as the ‘draft of the second act’). The entry into force of the draft of the second act has been delayed and, according to the latest information, the legislative procedure may not be completed before September 2018.

The two new pieces of legislation are aimed at implementing the GDPR into the Polish legal order, as well as regulating the matters in which the GDPR leaves a certain regulatory freedom for EU Member States. The new PDPA establishes a...
new supervisory body – the President of the Office for Personal Data Protection (hereinafter referred to as the ‘President of the Office’), which has a much wider range of powers than the previous DPA (Inspector General for the Protection of Personal Data – hereinafter referred to as the ‘Inspector General’).

The amendments to the sectorial regulations included in the draft of the second act will affect, among others, employment, banking and insurance regulations. The act is still going through the legislative procedure (the most recent draft was published on 7 June 2018) so the exact scope of the changes remains unclear.

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 new PDPA does not include any local derogations to the definitions set out in GDPR. The most recent draft of the second act also does not include any local derogations, however, it is still going through the legislative procedure and may be subject to change.

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 President of the Office for Personal Data Protection

(Office of the President for Personal Data Protection)
Biuro Prezesa Urzędu Ochrony Danych Osobowych
Stawki 2
00 193 Warsaw, Poland

Tel. (22) 531 03 00
Fax (22) 531 03 01
kancelaria@uodo.gov.pl

Helpline: tel. 606-950-000 is open from Monday to Friday from 10 am to 1 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 (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 previous PDPA (being in force until 25 May 2018), as a general rule, data controllers that process personal data were obliged 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 exist under the new PDPA.

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 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 address of the DPO and its national identification number (REGON) if the DPO is an economic entity. Any changes to the information provided or the dismissal of a DPO should also be notified within 14 days.

If a person/entity was appointed as an Information Security Officer (ABI) under the previous PDPA, this person/entity will automatically become a DPO for the data controller until 1 September 2018. If the appointment of a DPO is notified to the President of the Office before that date, the person/entity will continue 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 must take place and be notified to the President of the Office before 31 July 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 (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 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. 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.

The new PDPA includes some derogations from the GDPR. However, the draft of the second 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 draft of the second 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 and email monitoring. 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.

The remaining changes to the Labour Code are included in the draft of the second act.

For example the draft of the second act contains provisions which will allow the employer to process the personal data of its employees referred to in Article 9 section (1) and Article 10 of the GDPR only when necessary to perform an obligation imposed on the employer by law – any other legal grounds will not be accepted for this type of processing.

Please note that the whole draft of the second act is still going through the legislative procedure and is likely to be further amended.

**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.

In the case of the transfer of personal data to a third country, the new PDPA does not impose any additional requirements concerning notifications to or registrations with the President of the Office.

**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:

- 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

The new PDPA 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 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.
In Poland, data controllers from the telecommunications sector are required to inform sectoral regulators of any data security breach. Pursuant to the Telecommunications Act, the provider of telecommunications services is obliged to immediately (and no later than within three days of learning about a data breach) notify the President of the Office about any data breach. 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 immediately (and no later than within three days of learning about the data breach) also inform the subscriber or end user (in addition to informing the President of the Office) about the breach.


A personal data breach should be reported by the provider of telecommunications services to the President of the Office immediately, and no later than 24 hours after the detection of the personal data breach. This deadline results from Article 2 section (2) of the 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.

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 (and no later than within three days of learning about the data breach) inform the subscriber or end user (in addition to informing the President of the Office) about the breach under the terms specified in Regulation 611/2013.

Please note that the legislative procedure is still in progress and this matter should be reviewed again in due time.

**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 President of the Office is responsible for the enforcement of Polish data protection law and as such is entitled to carry out audits of data controllers in order to determine their compliance with the regulations on the protection of personal data and to impose administrative fines, by means of an administrative decision, pursuant to Article 83 of the GDPR.

The new PDPA provides for a lower level of fines that can be imposed on public authorities for breaching the GDPR – the maximum amount is PLN 100,000 (approx. EUR 25,000).

The new PDPA maintains the criminal liability for individuals who process personal data:

- A person who processes personal data where such processing is forbidden or where he/she is not authorized to carry out such processing may be liable to a fine, a partial restriction of freedom, or imprisonment of up to two years (or three years if special categories of personal data are processed)

- A person who prevents or hinders the performance of inspection activities conducted by the President of the Office (or its delegated inspectors) may be liable to a fine, a restriction of liberty, or imprisonment of up to two years.
As only individuals (and not legal entities) may be prosecuted for criminal offences, the person who may potentially face criminal charges would be a member of the management board (the person performing the role of data controller in a legal entity) or an employee authorized to process personal data (e.g., a data protection officer or human resources officer).

Currently, there is limited information on the practice of enforcement under GDPR in Poland.

**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, a change which is currently forecast for Spring 2019. 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 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 2017, item 1219, hereinafter referred to as the ‘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 – 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 addresses (such as office@company.com) and to a specific employee’s business email address (such as name.surname@company.com).

According to the current draft of the second 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 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 in progress and the matter should be reviewed again in due time.

**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/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).

**ONLINE PRIVACY**

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/her consent.

**Data about location**

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
- anonymise 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 authorised by a public telecommunications network operator
- are authorised 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/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; or
• 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; and
• 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/her monthly remuneration.

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 (ie subscriber or end user) gives his/her consent.

Location data

In order to use location data (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 location data concerning this user, which may be withdrawn for a given period or in relation to a given call, or
A provider of publicly available telecommunications services is obliged to inform the user, prior to receiving its consent, about the type of location data which is to be processed, 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 location data may only be performed by entities that:

- are authorised by a public telecommunications network operator
- are authorised by a provider of publicly available telecommunications services,
- provide a value-added service

Location data may only be processed 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/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 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, or
- 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; and
- gives its consent to the installation and use of the software prior to its installation.

According to the current draft of the second act, the consent of the subscriber or the end user must comply with the GDPR format requirements. The legislative procedure is still in progress and this matter should be reviewed again in due time.

**Enforcement and sanctions**

A company that processes transmission data contrary to the Telecommunications Act or fails to meet obligations to obtain consent to process location data 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/her monthly remuneration.

**KEY CONTACTS**

**Ewa Kurowska-Tober**  
Partner, Head of IPT  
T +48 22 540 74 1502  
ewa.kurowska-tober@dlapiper.com

**Łukasz Czynienik**  
Senior Associate  
T +48 22 540 74 67  
lukasz.czynienik@dlapiper.com

**DATA PRIVACY TOOL**

You may also be interested in our Data Privacy Scorebox to assess your organisation’s level of data protection maturity.
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 the draft GDPR implementation law is yet to be passed in the Parliament, it is anticipated that its publication will only occur after the GDPR application date.

In this scenario, the Personal Data Protection Law will remain in force after 25 May 2018 (i.e. the provisions that do not directly contradict the GDPR), which may, potentially, create some difficulties in the application of the new data protection legal regime until subsequent entry into force of the GDPR implementation law.
“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 Protection Law defines ‘personal data’ as any given information, in any format, including sound and image, related to a specific or an identifiable natural person (‘data subject’). An identifiable natural person is one who can be identified, directly or indirectly, namely by reference to a specific number or to one or more elements concerning his/her physical, physiological, mental, economic, cultural or social identity.

On the other hand, ‘sensitive personal data’ is defined as any personal data revealing one’s philosophical or political beliefs, political affiliations or trade union membership, religion, private life and racial or ethnic origin, and data concerning health or sex life, including genetic 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 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.
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 Personal Data Protection Law, as a general rule, data controllers who process personal data shall notify such activity to the Data Protection Authority ('CNPD'), unless a specific exemption applies. For instance, CNPD has issued decisions on the exemption of notification being applicable to activities related with salary processing, invoicing and client/supplier management, entry and exit of persons in buildings, among others.

For certain categories of data (sensitive data, data regarding unlawful activities or criminal and administrative offences or credit and solvability data) and certain types of processing, prior authorisation from the CNPD is required, with any variations or changes to the processing of personal data determining mandatory amendment of the registration.

Notification is made electronically through CNPD’s website by means of an official form including the following information:

- identity of the controller and its representative;
- purposes of the processing;
- third party entity responsible for the processing (data processor), if applicable;
- categories of entities to which the personal data is communicated, their identification and the purposes of communication if applicable;
- all the personal data that will be processed, being necessary to indicate if sensitive data will be collected, as well as data concerning the suspicion of illegal activities, criminal and/or administrative offences and data regarding credit and solvability;
- grounds for lawful processing and a brief description of the data collection method used;
- storage period: the way of exercising the right of access and rectification;
- combination of personal data, if applicable;
- available means and methods for updating the data;
- any transfers of data to third countries, including a list of such entities and countries, what personal data is transferred, reasons and respective grounds for the transfer and the measures adopted in each transfer; and
- physical and logical security measures implemented.
It should be noted that, when the GDPR enters into force, these provisions will most likely be considered tacitly revoked, as they contradict the Regulation and namely one of its main principles: the principle of accountability.

**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 current Personal Data Protection Law does not provide for the requirement of appointing Data Protection Officers. Therefore, until the application date of the GDPR, organisations are not required to appoint a data protection officer.

As regards the mandatory communication of the data protection officer to the supervisory authority, in the context of Article 37 (7) of the GDPR, there are still no defined procedures and/or mechanisms.

**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 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. 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 data may only be processed if the data subject has given his/her unambiguous consent or any of the lawfulness grounds are applicable.

Grounds for Lawful Data Processing are the following:

- execution of an agreement(s) where the data subject is party or in previous diligences for the conclusion of an agreement at the request of the data subject;
- compliance with a legal obligation that the controller is subject to;
- protection of vital interests of the data subject if the latter is physically or legally unable of giving his/her consent
- 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 is disclosed, or
- pursuing legitimate interests of the controller or the third party to whom the data is disclosed, except where such interests should be overridden by interests or fundamental rights, freedoms and guarantees of the data subject.

Moreover, the data controller must provide the data subject with all the relevant processing information, which includes the identity of the data controller, the purposes of processing, the recipients or categories of personal data and the means made available to the data subject to access, amend and delete its data.

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.

As regards data transfers performed within the EU/EEA countries, mandatory notification to the Data Protection Authority (‘CNPD’) is required and, in principle, data processing may commence immediately thereafter.

Transfers to non-EU/EEA countries can only take place if the recipient’s country ensures an adequate level of protection. In any case an authorisation procedure with the CNPD is mandatory and data processing can only commence once the authorisation is issued.

Exceptionally, transfers performed under specific circumstances are possible, notably according to Standard Model Clauses or to Privacy Shield Framework holders. In such cases, data processing can be done, in principle, immediately after filing with CNPD.

CNPD has issued specific guidelines on IntraGroup Agreements (IGA) involving transfers of personal data to non-EU/EEA countries and considers that such transfers are always dependant on its prior authorisation (assessing if a determined IGA presents sufficient guarantees).

When IGA agreements follow EU model clauses, although designed for bilateral relationships, CNPD understands that there are grounds to authorise the transfers in an expedite manner if the data controller declares that such agreement is identical and in accordance with EU model clauses.

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 controller must implement adequate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular when processing involves transmission of data over a network, and against all other unlawful forms of 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).

---

In Portugal, Comissão Nacional de Proteção de Dados (‘CNPD’) is responsible for the enforcement of the Personal Data Protection Law.

Failure to comply with data protection and privacy legal requirements and formalities may result in criminal, civil and administrative liability. Depending on the specific circumstances, criminal offenses may be punished with imprisonment up to 2 (two) years or fine up to 240 days and administrative offences may be punished with fine up to EUR 29,927.88.
The Personal Data Protection Law determines that any person who intentionally:

- fails to notify or seek CNPD’s authorisation for data processing;
- provides false information in the notification or applications for authorisation for the processing of personal data;
- misappropriates or uses personal data in an incompatible manner with the purpose of the collection or with the legalization document (e.g. contract);
- promotes or carries out an illegal combination of personal data;
- fails to comply with the obligations provided for in the Personal Data Protection Law or other data protection legislation within the time limit set by the CNPD for compliance; or
- continues to allow access to open data transmission networks to controllers who fail to comply with the provisions of this Act after notification by the CNPD not to do so, shall be subject to a penalty up to one year’s imprisonment or a fine of up to 120 days.

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, a change which is currently forecast for Spring 2019. 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, 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 e-mail 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/user’s terminal is only allowed if the subscriber/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/user.

Traffic Data

Traffic data must be erased or anonymised 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/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 anonymised 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@dlapiper.com
DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation's level of data protection maturity.
On 3 November 2016 the Qatari government passed a data protection law, Law No. (13) of 2016 Concerning Personal Data Protection (‘Data Protection Law’). The Data Protection Law will come into effect within six months of the date of issue, that is 3 May 2017 (unless this period is extended).

Qatar is the first GCC member state to issue a generally applicable data protection law.

The Data Protection Law envisages further regulations being issued to assist its implementation.

The Data Protection Law will apply to personal data when this data is processed electronically, or obtained, collected or extracted in any other way in preparation for the electronic processing thereof, or that is 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 and honesty and respect for human dignity, and acceptable practices 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 details of 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

Qatar Ministry of Transport and Communications (MoTC).

REGISTRATION

There is currently no requirement in Qatar for data controllers who process personal information to register with the regulator, the MoTC.

DATA PROTECTION OFFICERS

There is currently no obligation for organisations 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

Data controllers may collect and process personal data when the data subject consents, unless processing is deemed necessary for realising a ‘lawful purpose’ for the controller or for 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’.

Before commencing the processing of 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
- The data processing is required to meet a legal obligation
- The data processing is required to protect the data subjects vital interests
- The data processing is required for scientific research being conducted in the public interest, and
- 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 authorisation from the MoTC. The procedure for obtaining this authorisation has not yet been issued (this is likely to be in the form of a Ministerial resolution).

TRANSFER

Data controllers may collect, process and transfer personal data when the data subject consents, unless deemed necessary for realising 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 organisation 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 to report any violation of the same with the aim of safe guarding personal data
- Adopt suitable technical means to enable individuals to practice their rights to access, review, and correct personal data in a direct way
- 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. Organisations should adopt best practise methodologies in keeping with their business sector.

BREACH NOTIFICATION

There is an obligation on the data controller to notify the regulator, the MoTC and the data subject of any breaches of the measures to protect the data subjects privacy if it is likely to cause damage to the data subject.

ENFORCEMENT

In Qatar, the MoTC is responsible for the enforcement of the Data Protection Law. Any data subject may submit a complaint to the MoTC in the case of a violation of the Data Protection Law. The MoTC will investigate the complaint and if found to be valid the MoTC can oblige the data controller or processor to rectify the violation within a specified time period.

The MoTC can also impose fines of up to QAR 5,000,000 (USD 1,400,000) for violations of the Data Protection Law.

ELECTRONIC MARKETING

Communications made electronically (including by wired or wireless communication) are prohibited under the Data Protection Law, where their purpose is unsolicited direct marketing. Electronic communications for the purposes of direct marketing are therefore only permitted only with the consent of the recipient.

The approved electronic communications must include the identity of the sender and an indication that it is sent for the purposes of direct marketing. The message must include an address that can easily be reached and 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 (or any other law) does not specifically regulate on-line privacy or the use of cookies and location data except in relation to children. Owners and operators of websites must observe the followings requirements:

- 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

- Making a 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, is prohibited.

**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 organisation’s level of data protection maturity.
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 legislative proposal regarding the implementing measures for Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (GDPR) (the 'Draft Law') was sent to the Legal Committee of the Chamber of Deputies for debate and registered under no. 4c-11/36 as of 11 April 2018.

The purpose of the Draft Law is to ensure the applicability of certain provisions of the GDPR in Romania, also considering that Law no 677/2001 on the protection of individuals with regards to the processing of personal data and the free movement of such data ('Data Protection Law') shall be repealed on 25 May 2018. The Draft Law includes provisions with respect to the following specific areas:

- determining the processing conditions of certain categories of personal data or for certain purposes
- the framework related to the sanctions applicable to public authorities and public bodies in Romania
- the introduction of additional conditions, including restrictions with respect to the processing of genetic data, biometric data, health data, for the purpose of achieving an automated decision-making process or the creation of profiles, taking into account the risks involved by the use of such data.

The Draft Law was approved by the Legal Committee of the Chamber of Deputies and was sent to the Chamber of
Deputies for approval.

The Draft Law has now been approved by the Romanian Parliament and awaits final approval by the President. The law will soon become applicable but we do not have a precise date. It is expected to be published shortly.

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 Draft Law does not provide any specific definitions with respect to "personal data", as this is 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;
- "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 the (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 the time period comprised between 60 and 180 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 in the Draft Law.

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.

**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.

Starting with 25 May 2018 when the GDPR becomes applicable, any registration obligations with ANSPDPC are 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 addition to the requirements provided by the GDPR in Articles 37 to 39, the Draft Law 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 (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 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 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 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. 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.

1. Processing of 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 of the controller to implement adequate measures. The Draft Law does not specify or provide any examples with respect to
what type of measures should be implemented by the controller in view of the processing.

The Draft Law expressly allows the processing of health data under Regulation (EC) 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 and by third parties.

2. Processing a national identification number - The Draft Law provides that processing of 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:

a. 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;
b. the appointment of a DPO;
c. establishment of a retention policy 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 for deletion; and
d. regular training of the personnel that handles personal data processing activities.

3. Processing of 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 permitted only if:

a. the legitimate interests pursued by the employer are thoroughly justified and which prevail over the interests or rights and freedoms the targeted employees;
b. the employer has made the compulsory, complete and explicit prior information to the employees;
c. the employer consulted the relevant trade union or, where applicable, the employees’ representatives prior to the introduction of the monitoring systems;
d. other less intrusive forms and ways to achieve the goal pursued by the employer have not previously proved their effectiveness; and
e. the retention duration of personal data is proportional to the purpose of processing, but not more than thirty (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 the Draft Law, in view of ensuring a balance between the right of 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:

a. Chapter II - Principles;
b. Chapter III - Rights of the data subject;
c. Chapter IV - Controller and processor;
d. Chapter V - Transfers of personal data to third countries or international organizations;
e. Chapter VI - Independent supervisory authorities;
f. Chapter VII - Cooperation and consistency; and
g. Chapter IX - Provisions relating to specific processing situations.

5. Processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or
statistical purposes - According to the Draft Law Articles 15, 16, 18 and 21 of the GDPR do not apply in case personal data are processed for archiving purposes in the public interest, 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.

6. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. These safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. These measures may include pseudonymisation provided that those purposes can be fulfilled in that manner.

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 specific provisions / derogations are provided by the Draft Law with respect to personal data transfers.
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.

No specific provisions / derogations are provided by the Draft Law 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" (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 specific provisions / derogations are provided by the Draft Law with respect to the notification of a personal data security breach.

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).

ANSDPCD is entitled to investigate any breach of the GDPR provisions ex officio or following a complaint filed by a prejudiced data subject. In this sense, ANSDCP may perform an audit over data processing activities performed by data controllers.

The Draft Law provides specific rules with respect to enforcement. Specifically, ANSDCP may issue written warnings and apply fines.

Misdemeanours committed by public authorities/bodies, are generally sanctioned with a fine ranging between RON 10,000 (approx. EUR 2,222) to RON 200,000 (approx. EUR 44,444).

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, a change which is currently forecast for Spring 2019. 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 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 506/2004”). According to this law, it is forbidden to send commercial communications by using automatic systems that do not require the intervention of a human operator, by fax or electronic mail or any other similar method, except where data subjects have expressly consented in advance. It may be considered that SMS marketing falls under the same restrictions.

Moreover, cases where the data controller has directly obtained the e-mail address of a data subject upon the sale or provision of a certain service towards the latter, the controller may use the respective address for the purpose of sending electronic communications regarding similar products or services, provided that data subjects are clearly and expressly offered the possibility to oppose by way of an easily accessible and free of charge method, not only when the e-mail address is collected but also with each commercial communication received by the data subject.

ONLINE PRIVACY

The processing of traffic data, location data and the implementation of cookies are dealt with under Law 506/2004.

Traffic data
Traffic Data relating to subscribers and users processed and stored by the provider of a public 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 as of 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. 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 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. Data subjects may withdraw their consent at any time. The provider of electronic communication services must inform data subjects in respect of the processed traffic data, and the duration of processing, prior to obtaining their consent.

Communication service providers and entities acting under their authority may process traffic data 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 is permitted only if it is necessary to fulfil such purpose.

Location data - The processing of such data is permitted in each of the following instances:

- data is rendered anonymous
- data subjects have consented to such processing for the duration necessary for the performance of value added services, or
- when the purpose of the value added service is the unidirectional and non differentiated transmission of information towards users.

The service provider 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, communication service providers must grant users the possibility, using a simple means and free of charge, 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:

- users have expressly consented thereto (Law 506/2004 also provides that consent may be given by way of browser settings or other similar technologies), and
- 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 users’ computer terminal, they 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 506/2004 is classified as a minor offence and is sanctioned with fines ranging from EUR 1,120 to EUR 22,500. In the case of companies whose turnover exceeds approximately EUR 1,120,000,
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 electronic communication services offered to the public and providers of electronic communication public networks shall make available, as soon as possible, but no later than 48 hours, traffic data, data regarding user terminals, as well as geo location data.

**KEY CONTACTS**

**Ana-Maria Andronic**  
Head of Intellectual Property and Technology  
T +40 372 155 816  
anamaria.andronic@dlapiper.com

**Andrei Stoica**  
Junior Associate  
T +40 372 155 870  
andrei.stoica@dlapiper.com

**Paul Babus**  
Junior Associate  
T +40 372 155 883  
paul.babus@dlapiper.com

**DATA PRIVACY TOOL**

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

LAW

Fundamental provisions of data protection law in Russia can be found in the Russian Constitution, international treaties and specific laws. Russia is a member of the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention) (ratified by Russia in 2006) and the Russian Constitution establishes the right to privacy of each individual (articles. 23 and 24). Most rules are found in specific legislation, particularly the Data Protection Act No. 152 FZ dated 27 July 2006 (DPA) and various regulatory acts adopted to implement the DPA as well as other laws, including the Information, Information Technologies and Information Protection Act No. 149 FZ dated 27 July 2006 establishing basic rules as to the information in general and its protection. In addition, the Russian Labour Code contains provisions on the protection of employees’ personal data (Part XIV). Other laws may also contain data protection provisions which implement the provisions of DPA in relation to specific areas of state services or industries.

On 22 July 2014 notable amendments to the DPA were adopted and came into force on 1 September 2015. The amendments require all personal 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. A Register of Infringers of Rights of Personal Data Subjects shall be established by the Roscomnadzor and from there and the Roscomnadzor may move to block websites.

As the amendments are newly passed and a track record of enforcement and legal interpretation has not been established, it is still unclear as to how this register and the website blocking would work in practice. According to clarifications of Russian regulators, storing and processing of personal data of Russian individuals outside of Russia can still be compliant with the law as long as primary (often interpreted as initial) storage and processing of data is done in Russia. It is still an open question whether keeping "mirror" databases in Russia and elsewhere would be deemed as compliant.

DEFINITIONS

Definition of personal data

Personal data is defined in law as any information that relates directly or indirectly to the 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 and biometrical data.

NATIONAL DATA PROTECTION AUTHORITY

Federal Service for Supervision of Communications, Information Technologies and Mass Media or, in short, Roscomnadzor
REGISTRATION

The Agency is in charge of maintaining the Registry of Data Controllers.

Any data controller shall notify the Agency in writing about its intention to process personal data, unless one of the following exclusions applies:

- the personal data is exclusively data about employees;
- the personal data was received in connection with a contract entered into with the data subject, provided that such data is not transferred without the consent of the data subject, but used only for the performance of the contract and entering into contracts with the data subject (for example, data provided by a customer purchasing a product online and the data is used only to fulfil the order);
- the personal data is the data about members of a public or religious association and processed by such an organisation for lawful purposes in accordance with their charter documents, provided that such data is not transferred without the consent of the data subjects;
- the personal data was made publicly accessible data by the data subject;
- the personal data includes the surname, name and father’s name only (Russia uses patronymic references in place of "middle" names);
- the personal data is necessary in order to give single access to the premises of the data controller or for other similar purposes;
- the personal data is included in state automated information systems or state information systems created for the protection of state security and public order;
- the personal data is processed in accordance with the law without any use of automatic devices; or
- the personal data is processed in accordance with transportation security legislation for the purposes of procurement of stable and secure transport complex and personal, community and state interests protection.

The notification letter shall contain information about:

- the full name and address of the data controller;
- the purpose of the processing;
- the categories of personal data processed;
- the categories of the subjects whose personal data is processed;
- the legal grounds for processing;
- the types of processing of the personal data;
- the measures of protection of personal data;
- name and contact information of the physical person or legal entity responsible for personal data processing;
- the commencement date;
- information on occurrence of cross border transfer of personal data;
- the term of processing or the conditions for termination of processing the personal data; and
- information on personal data security provision.

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 advisable 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 controllers may collect and process personal data where any of the following conditions are met:

- the data subject consents;
- the processing is required by a federal 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 controller needs to process the data to perform or conclude a contract to which the data subject is a party or 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 impersonalised;
- the processing protects the data controller’s vital interests and it is impossible to have the data subject’s consent;
- the processing is required for execution of statutory controller’s or third parties’ rights or for purposes important for the community provided the data subject’s rights are not in breach;
- personal data that is processed was publicly made accessible by the data subject or upon his or her request;
- the processing is carried out by a journalist or mass media as a part of its professional activities or for the purposes of scientific, literary or other creative activities, except if the processing would damage the data subject’s rights and freedoms; or
- personal data that is processed is subject to publication or mandatory disclosure under law.

As a general rule, consents by a data subject may be given in any form, but it is the data controller’s obligation to provide proof that he has the data subject’s consent. Because of this burden of proof, it is important to keep careful records of consents.

In the following cases, the DPA requires that the data subject’s consent should be in writing (preferably in hard copy form):

- where the personal data is collected to be included within publicly accessible sources;
- where sensitive or biometrical data is processed;
- in the case of the cross border transfer of personal data, where the recipient state does not provide adequate protection of personal data; or
- where a legally binding decision is made solely on the grounds of the automated processing of personal data.

Consent is deemed to have been given in writing where it is signed by hand or given in an electronic form and signed by an electronic signature.

Consent may be revoked.

Consent in writing must contain the following information:

- the identity of the data subject, his/her address and passport details and identity of the subject;
- data representative (if any);
- the identity and address of the data controller or the entity that processes personal data on behalf of the data controller (if any);
- the purpose of the processing;
• the list of personal data that may be collected and processed;
• the types of processing that are authorised;
• the term for which the consent remains valid and way of revocation; and
• the data subject’s signature.

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.

TRANSFER

Prior to a transfer of personal data out of Russia, the data controller must ensure that the recipient state provides adequate protection of personal data. The fact that the recipient state ratified the Convention is sufficient grounds to deem that the state provides adequate protection of personal data for the purposes of the DPA.

Where there is no adequate protection of personal data, a cross border transfer is permitted if one of the following conditions is met:

• the data subject consents;
• the transfer is provided for under an international treaty to which Russia is a signatory;
• the transfer is necessary in accordance with federal laws for protection of the Constitution, state defence, security and transport system;
• for the purposes of performance of a contract to which the data subject is party; or
• the transfer protects the data subject’s vital interests where it is not possible to get the written consent of the data subject.

In addition to the above, the Roscomnadzor 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.

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

There is no mandatory requirement to report data security breaches or losses to the Agency or to data subjects.

ENFORCEMENT

In Russia, the Agency is responsible for the enforcement of the DPA. The Agency 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;
• initiate criminal cases; and
• impose administrative liability.

If the Agency becomes aware that a data controller is in violation of the law, he can serve an enforcement notice requiring the
A data controller can face civil, administrative or criminal liability if there is a violation of personal data law. Officers of the data controller responsible for the offence may also face disciplinary action.

Usually, in the case of violation of data protection law, the Agency will serve an enforcement notice requiring the position to be rectified and may also impose an administrative penalty and/or recommend imposing disciplinary action on the officers of the data controller who are responsible for the offence.

The maximum administrative penalty that can be imposed, as at the date of this review, is RUR (Russian Rubles) 75,000.

**ELECTRONIC MARKETING**

Electronic marketing activities are subject to limitations set by the Russian Law on Advertising No. 38-FZ dated 13 March 2006, under which the distribution of advertising through telecommunications networks, in particular, through the use of telephone, facsimile and mobile telephone communications, is allowed only subject to preliminary consent of a subscriber or addressee to receive advertising.

Advertising is presumed to be distributed without preliminary consent of the subscriber or addressee unless the advertising distributor can prove that such consent was obtained. The advertising distributor is obliged immediately to stop distribution of advertising to the address of the person who made such a demand.

**ONLINE PRIVACY**

Russian law does not specifically regulate online privacy. The definition of personal data under the DPA is rather broad and there are views that information on number, length of visits of particular web-sites and IP address (in combination with other data allowing the user to be identified) could be considered personal data.

**KEY CONTACTS**

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Contact Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Michael Malloy</td>
<td>Counsel and Head of Intellectual Property and Technology Practice</td>
<td>T +7 495 221 4400 <a href="mailto:michael.malloy@dlapiper.com">michael.malloy@dlapiper.com</a></td>
</tr>
<tr>
<td>Pavel Arievich</td>
<td>Legal Director</td>
<td>T +7 495 221 4472 <a href="mailto:pavel.arievich@dlapiper.com">pavel.arievich@dlapiper.com</a></td>
</tr>
<tr>
<td>Ekaterina Golodinkina</td>
<td>Associate</td>
<td>T +7 495 221 4546 <a href="mailto:ekaterina.golodinkina@dlapiper.com">ekaterina.golodinkina@dlapiper.com</a></td>
</tr>
</tbody>
</table>

**DATA PRIVACY TOOL**

You may also be interested in our Data Privacy Scorebox to assess your organisation’s level of data protection maturity.
SAUDI ARABIA

LAW

Shari’a principles (that is, Islamic principles derived from the Holy Quran and the Sunnah, the latter being the witnesses’ sayings of the Prophet Mohammed), which although not codified, are the primary source of law in the KSA. In addition to Shari’a principles, the law in the KSA consists of secular regulations passed by government, which is secondary if it conflicts with Shari’a principles.

At this time, there is no specific data protection legislation in place in the KSA (although we understand that a new freedom of information and protection of private data law is under review by the Shura Council). Shari’a principles generally protect the privacy and personal data of individuals.

That said, there are certain secular regulations passed by government, which although not dedicated as a whole to data privacy/protection, contain specific provisions governing the right to privacy and data protection in certain contexts. Examples of such regulations include:

- the Basic Law of Governance (no: A/90 dated 27th Sha’ban 1412 H (corresponding to 1 March 1992)), which provides that telegraphic, postal, telephone and other means of communications shall be safeguarded. They cannot be confiscated, delayed, read or breached

- the Anti-Cyber Crime Law (8 Rabi 1, 1428 (corresponding to 26 March 2007)) (as amended), which generally prohibits, amongst other things, the interception of data transmitted through an information network, the invasion of privacy through the misuse of camera-equipped mobile phones and the like, illegally accessing bank or credit data of another, unlawful access to computers for the purpose of deleting, destroying, altering or redistributing private data, or the production, preparation, transmission or storage of material impinging on public order, religious values, public morals, and privacy, through an information network or computers;

- the Telecoms Act (approved pursuant to the Royal Decree No. (M/12) dated 12/03/1422H (corresponding to 3 June 2001), which states that the privacy and confidentiality of telephone calls and information transmitted or received through public telecommunications networks shall be maintained, and disclosure, listening or recording the same is generally prohibited

- the Regulations for the Protection of Confidential Commercial Information (issued by Minister of Commerce and Industry Decision No. (3218) dated 25/03/1426H (corresponding to 4 May 2005), and as amended), which governs the protection of data considered to be "commercial secrets" under these regulations.

There may also be specific regulations applicable to certain industries, for example, in banking, the Saudi Arabian Monetary Agency imposes a general duty of confidentiality on banks, and requires banks to provide a safe and confidential environment to ensure confidentiality and privacy of customer data. Similarly, in the healthcare sector, confidentiality requirements will apply in terms of protecting medical data of patients.
In the absence of specific regulations which apply, the courts will apply Shari’a principles, which in essence provide that an individual has a right to be compensated for losses/harm suffered as a result of the disclosure of his/her personal information and/or breach of privacy by another party. A KSA court may also, in its absolute discretion, impose other penalties on a case by case basis (for example, imprisonment and/or fines).

DEFINITIONS

Definition of personal data

In the absence of specific data protection legislation, there is no definition of "personal data".

Definition of sensitive personal data

In the absence of specific data protection legislation, there is no definition of "sensitive personal data".

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in the KSA. In respect of telecommunications services, the Communications and Information Technology Commission (‘CITC’) is responsible for overseeing the relevant telecoms laws and policies. The Saudi Arabian Monetary Agency is responsible for, amongst other things, overseeing commercial banks in the KSA.

REGISTRATION

In the absence of a national data protection authority, there are no data protection registration requirements in the KSA.

DATA PROTECTION OFFICERS

There is no requirement in the KSA for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

There is no concept of "data controller" or "data processor" in the KSA. To ensure compliance with Shari’a, it is advisable to obtain data subjects’ consent before processing their data.

TRANSFER

There are generally no specific data protection regulations regarding transfer of data outside of the KSA, although in certain sectors, the approval of a regulatory authority may be required. We do generally recommend that consent is sought from data subjects for any processing or transfer of personal data outside of the KSA.

SECURITY

There are no specific security measures that must adopted and implemented by commercial organisations, although as a matter of best practice and to avoid unauthorised processing, disclosure, loss or theft of personal data (and therefore potential liability under Shari’a), it is recommended that appropriate measures (technical and organisational) are put in place to protect the personal data held.

BREACH NOTIFICATION

There are no data protection regulations imposing a mandatory requirement to report data security breaches.

ENFORCEMENT

At this time, there is no clear designated authority responsible for the enforcement of data protection and privacy equivalent to, say, the Information Commissioner in the United Kingdom. That said, specific authorities are tasked with enforcing breaches of other legislation that is in place (for examples of such legislation, please see the section above entitled 'LAW'). For example, under
the Anti-Cyber Crime Law (as amended), the Bureau of Investigation and Public Prosecution is tasked with carrying out investigations, with the CITC providing any technical support required, and the matter potentially being referred to the courts.

**ELECTRONIC MARKETING**

Electronic marketing is regulated by Spam Regulations issued by the CITC, which require, amongst other things, opt-in consent from the date subject to receive electronic messages.

**ONLINE PRIVACY**

There is no specific legislation in the KSA that expressly regulates the use of cookies. We generally recommend that the use of cookies should be carefully and fully disclosed in a website privacy policy (which should be compliant with KSA law).

**KEY CONTACTS**

Mohamed Moussallati  
Legal Consultant  
T +966 11 201 8900  
mohamed.moussallati@dlapiper.com

**DATA PRIVACY TOOL**

You may also be interested in our [Data Privacy Scorebox](http://www.dlapiperdataprotection.com) to assess your organisation’s level of data protection maturity.
SERBIA

LAW


However, the Ministry of Justice prepared a draft of a new Law on Protection of Personal Data in November 2017, with the general objective of harmonizing the Serbian data protection law with the General Data Protection Regulation (“GDPR”). The public discussion regarding this draft Law commenced on 1 December 2017 and lasts until 15 January 2018. The Serbian Minister of Justice has stated that the expected timeframe for the adoption of this new draft Law and the commencement of its implementation is by May 2018. The final version of this draft law and whether/when exactly it will be adopted and implemented remains to be seen.

DEFINITIONS

Definition of personal data

Under the DP Law, personal data is any information on a natural person based on which the respective person is identified or identifiable (for example, name, address, e-mail 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 znaaja i zaštitu podataka o linosti) (“DPA”).

It is seated at Bulevar kralja Aleksandra 15 Belgrade and its website is www.poverenik.rs.

REGISTRATION

Any person or legal entity which processes personal data in Serbia (and, based on the relevant processing, establishes a database containing personal data) has to report the relevant processing to the DPA (i.e. has to register both the respective database and itself as the data controller).

This database registration obligation generally consists of two phases – the first one is to notify the DPA of the intention to establish a database (at the latest 15 days prior to the intended database establishment date) and the second one is to report to the DPA that the respective database was created (at the latest 15 days from the date of its creation). Both phases are performed by filing prescribed forms with the DPA (both on-line through the so-called Central Register of the DPA and in hard copy via post); the respective forms contain specific data on the data controller (such as its name and address of its registered seat) and on the database itself (for example, the purpose of and legal ground for its establishment, identification of exact processing activities,
types of processed data, categories of data subjects, etc.). Any subsequent change of the registered database (for example, change of the initially registered processing activities) has to be reported to the DPA as well, at the latest 15 days from the date when the particular change occurred.

**DATA PROTECTION OFFICERS**

There is no statutory obligation for an entity which processes personal data to have a data protection officer.

**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 there are a few cases when a data subject’s personal data may be processed without the data subject’s consent (for example, when the processing is necessary for fulfilment of the data controller’s statutory obligations or for preparation or realisation of an agreement concluded between a data controller and data subject) (“Exceptional Cases”).

Apart from the Exceptional Cases, consent is a precondition for legitimate collection and processing of personal data, and must be informed consent, meaning that it 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 of the processing, identification of exact processing activities, information on other users of the data in cases when the data controller is not its only user, information on statutory rights of the data subjects in relation to the respective processing, etc.)

Moreover, although consent is necessary, 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).

**TRANSFER**

The rules on the transfer of personal data, as envisaged by the DP Law, are quite general. Under the respective rules, there are two regimes for data transfer out of Serbia depending on whether the transfer will take place with or without the DPA’s prior approval. The determining factor is whether a country to which the data is to be transferred is a member state of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (“Relevant Convention”). If a country to which the data is to be transferred has signed and ratified the Relevant Convention (such as, for example, the EU countries), the transfer from Serbia is free in the sense that it is not conditional upon prior data transfer approval of the DPA (“Transfer Approval”), otherwise, Transfer Approval is necessary (such as, for example, for a transfer to the US).

In addition to the above, it should also be noted that the DPA’s position regarding data transfer out of Serbia is very strict, and, thus, the procedure for obtaining the Transfer Approval (which is initiated by a written request submitted to the DPA by the Serbian entity which intends to transfer the data out of the country) is very complex and time consuming and the outcome is rather uncertain.

**SECURITY**

There are no specific security measures prescribed by the DP Law. It is only generally prescribed that:

- personal data must be adequately protected from abuse, destruction, loss, unauthorised alterations or access; and
- both data controllers and processors are to undertake all necessary technical, human resources and organisational measures to protect data from loss, damage, inadmissible access, modification, publication and any other abuse, as well as to provide for an obligation of keeping data confidentiality for all persons who work on data processing.

**BREACH NOTIFICATION**

The DP Law does not impose a duty to notify a data security breach. However, it should be mentioned, for the sake of
completeness, that the Law on Electronic Communications ('Official Gazette of the Republic of Serbia', nos. 44/2010, 60/2013 and and 62/2014) ("EC Law") imposes a duty on entities which are operators of public communication networks and publicly available electronic communication services ("Operators") to notify the Regulatory Agency 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 has influenced their work significantly, and particularly on the breaches which resulted in violation of protection of personal data or privacy of the respective networks/services' users/subscribers.

Non performance of this statutory obligation can lead to offence liability and fines ranging from approx. EUR 4,098.00 to EUR 16,393.00 for a legal entity, and in range from approx. EUR 410.00 to EUR 1,230.00 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 (3) years, and, for a responsible person in a legal entity, a prohibition against performing certain duties for a duration of up to one (1) year).

ENFORCEMENT

The DPA is responsible for the enforcement of the DP Law. Namely, the DPA is authorised and obliged to monitor whether the DP Law is implemented and it conducts such monitoring both ex officio 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:

- order the data controller to eliminate the existing irregularities within a certain period of time;
- temporarily forbid particular processing; or
- 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 behaviour 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 monetary fines (ranging from approx. EUR 410.00 to EUR 8,197.00 for a legal entity and from approx. EUR 41.00 to EUR 410.00 for a responsible person in a legal entity).

Moreover, 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 monetary fine (of an amount to be determined by the court) or imprisonment of up to one (1) year. Both natural persons and legal entities can be subject to the respective liability.

ELECTRONIC MARKETING

Electronic marketing is not governed by the DP Law. The rules on this subject are envisaged by the Law on Electronic Trade ('Official Gazette of the Republic of Serbia', nos. 41/2009 and 95/2013), EC Law (as defined above in the section on Breach Notification), the Law on Advertising ('Official Gazette of the Republic of Serbia', no. 6/2016) and the Consumer Protection Law (Official Gazette of the Republic of Serbia, nos. 62/2014 and 6/2016) (together, the "Relevant Legislation").

In brief, based on the Relevant Legislation, electronic marketing is only allowed if it is covered by an explicit, prior written 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); and
- provided with a way to opt out of future marketing messages, at any time and free of charge.

ONLINE PRIVACY

There are no specific regulations explicitly governing on-line privacy (including cookies). Accordingly, the general data protection rules, as introduced by the DP Law, are, to the extent applicable, relevant for on-line 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, which are obligatory for entities which are the Operators (as defined above in the section on Breach Notification). Under these rules, the Operators are allowed:

- to process traffic data only as long as such data is necessary for a communication’s transmission and thus, when such necessity ceases to exist, the Operators are obliged, unless exceptionally (for example, in the case when they have obtained prior consent of the data subjects for using the respective data for marketing purposes), to delete such data or to keep them but only if they make the persons to which the date relates unrecognisable; and
- to process location data generally only if the persons to which the data relates are made unrecognisable or if they have such persons’ prior consent for the purpose of providing them with value added services (but even if such consent does exist, only in the scope and for the time during which the processing is needed for the respective purpose’s realisation).

Violations are subject to the fines set forth above in the Breach Notification section.

**KEY CONTACTS**

Karanovic & Nikolic

www.karanovic-nikolic.com/

Sanja Spasenovic
Attorney at law in cooperation with Karanovi & Nikoli
T Office +381 11 3094 200/ Direct T +381 11 3955 413
Sanja.Spasenovic@karanovic-nikolic.com

**DATA PRIVACY TOOL**

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

LAW

The Data Protection Act (the 'Act') was enacted in 2003 (Act No. 9 of 2003) with the aim of protecting the fundamental privacy rights of individuals against the use of data concerning them without their informed consent. The Act will come into operation on such date as the Minister notifies in the official Gazette.

As of May 2015, the Act has not yet come into operation.

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
Senior Associate
T +230 208 5526
shalinee.dreepaul-halkhoree@dlapiper.com

Arvin Halkhoree
Barrister
T +(230) 208 5526
ahalkhoree@juristconsult.com

DATA PRIVACY TOOL

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

Singapore enacted the Personal Data Protection Act 2012 (No. 26 of 2012) (‘Act’) on 15 October 2012. The Act took effect in 3 phases:

1. provisions relating to the formation of the Personal Data Protection Commission (the ‘Commission’) took effect on 2 January 2013;
2. provisions relating to the National Do-Not-Call Registry (‘DNC Registry’) took effect on 2 January 2014; and
3. the main data protection provisions took effect on 2 July 2014.

The Act has extraterritorial effect, and so applies to organisations collecting personal data from individuals in Singapore whether or not the organisation itself has a presence in Singapore.

The data protection obligations under the Act do not apply to the public sector, to whom separate rules apply.

The Commission’s first public consultation reviewing the Act (“PDPA Consultation”) closed in October 2017, and focused on ‘approaches to managing personal data in the digital economy’, with topics including ‘challenges for alternatives to consent’ and mandatory breach notification.

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
- from that data and other information to which the organisation 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 dead for 10 years or fewer.

The data protection obligations under the Act do not apply to "business contact information" (including name, position name or title, business telephone number, business address, business electronic mail address or business fax number) provided solely for business purposes, though 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 (i.e. both for business and personal purposes), the Act should be adhered to.

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 discretely, for limited purposes and the security measures afforded to such data should take into account the sensitivity of the data. The Commission has also stated in its enforcement decisions that the fact that personal data is of a sensitive financial nature is a relevant factor in its decisions, and a public condition in 2017 proposed draft additional safeguards for collection, use and disclosure of NRIC numbers.

**NATIONAL DATA PROTECTION AUTHORITY**

Personal Data Protection Commission

460 Alexandra Road  
#10-02 PSA Building  
Singapore 119963

T +65 6377 3131  
F +65 6273 7370

info@pdpc.gov.sg  
http://www.pdpc.gov.sg/

**REGISTRATION**

There are no registration requirements under the Act.

While not a requirement, in April 2017 the Commission publicly encouraged organisations to register their Data Protection Officers ("DPOs") with the Commission via the Commission’s website, to assist DPOs to keep up to date with development in the law.

**DATA PROTECTION OFFICERS**

Each organisation must appoint one or more data protection officers to be responsible for ensuring the organisation’s compliance with the Act. An organisation 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 organisation. The business contact information of the DPO must be made available to the public.

While there is no requirement for the data protection officer to be a citizen or resident in Singapore, the Commission suggests that the data protection officer 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 data protection officer may lead to a preliminary investigation by the Commission. If an organisation 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 S$10,000 or imprisonment for a term not exceeding 12 months, or to both. An organisation may be subject to a fine of up to S$100,000.

**COLLECTION & PROCESSING**

Organisations may only collect, use or disclose personal data where:

- 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 etc.) to the individual on or before collecting, using or disclosing the personal data; or

- there is deemed consent by the individual to the collection, use, or disclosure of the personal data in accordance with the
  relevant conditions of the Act; or
- if no consent or deemed consent is given, if limited specific exclusions prescribed in the Act apply.

An individual may at any time withdraw any consent given, or deemed given under the Act, upon giving reasonable notice to the
organisation.

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 organisation must also:

- make information about its data protection policies, practices and complaints process publicly available;
- cease to retain personal data or anonymise it where it is no longer necessary for any business or legal purpose; and
- ensure personal data collected is accurate and complete if likely to be used to make a decision about the individual or
disclosed.

There are transitional "grandfathering" arrangements for personal data collected prior to the data protection obligations in the Act
coming into full force on 2 July 2014.

New data protection management programme ("DPMP") and data protection impact assessment ("DPIA") guides were published
by the Commission in November 2017.

**TRANSFER**

In disclosing or transferring personal data to third parties (including affiliates), an organisation 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).

The Act also contains offshore transfer restrictions, which require an organisation to ensure "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 recently released guidance, including model clauses);
the individual has given consent (and provided required notices have been provided); and where transfers are considered
necessary in certain prescribed circumstances (which include in connection with performance of contracts between the
transferring organisation and the individual, subject to certain conditions being met). An organisation 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 Commission has published a new guide to data sharing (covering intragroup and third party sharing) with practical nonbinding
guidance for organisations, as well as DPMP and DPIA guides (see "Collection and Processing" above).

**SECURITY**

Organisations must protect personal data in their possession or under their control by making reasonable security arrangements
to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. 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.

A draft Cybersecurity Bill was published by the Singaporean authorities in 2017 ("Cybersecurity Bill"), following a public
consultation, which (if passed) potentially impacts data security measures and data breach incident handling, so organisations are
advised to monitor developments.
BREACH NOTIFICATION

Currently, there are no mandatory requirements under the Act for data users to notify the Commission or individuals regarding data protection breaches in Singapore. The Commission issued a best practice guide in May 2015 to help organisations manage personal data breaches effectively, and more recent guidelines provide practical tips on avoiding and managing risks such as accidental data disclosure. It is recommended that affected individuals be notified immediately if a data breach involves sensitive personal data. The Commission should be notified as soon as possible of any data breaches that might cause public concern or where there is a risk of harm to a group of affected individuals. Aggrieved parties may either make a complaint to the Commission, or may take out a private action in civil proceedings. The Commission may also conduct investigations on its own motion.

However the PDPA Consultation and the Cybersecurity Bill mean there are now draft proposals to introduce mandatory data breach notifications in Singapore, so organisations are advised to monitor developments.

ENFORCEMENT

Enforcement of the Act is carried out by the Commission. The powers of the Commission include giving directions to:

- 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; and/or
- pay a financial penalty not exceeding S$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 published the *Advisory Guidelines on Enforcement of Data Protection Provisions* in April 2016. These guidelines 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; co-operation 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:

- a point of law arising from a direction or decision of the Appeal Committee; or
- 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 lie 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; and/or
- 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 organisation 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 organisation 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; must not be a condition for supplying goods, services, land, interest or opportunity; and must not be obtained through the provision of false or misleading information or through deceptive or misleading practices. In the absence of such consent, organisations must check and ensure that the telephone number is not on a Do-Not-Call register maintained by the Commission (‘DNC Register’), unless such checks are exempted under the Act. 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 message. An individual may at any time apply to the Commission to add or remove his Singapore telephone number on the DNC Register.

The Act will apply to marketing messages addressed to a Singapore telephone number where:

- the sender of the marketing message is present in Singapore when the message was sent, or
- 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 (Cap 311A), 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.

**ONLINE PRIVACY**

Currently, there are no specific requirements relating to online privacy (including cookies and location) under the Act. Nevertheless, an organisation 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 organisation 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 the Collection & Processing chapter. The Commission has published nonbinding guidelines providing practical tips on pertinent topics such as securing electronic personal data and building websites, and a public consultation as 'approaches to managing personal data in the digital economy' was undertaken by the Commission in Summer 2017.

**KEY CONTACTS**

Scott Thiel
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group
T +852 2103 0519
scott.thiel@dlapiper.com

**DATA PRIVACY TOOL**

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

As a member of the European Union, Slovakia implemented the EU Data Protection Directive 95/46/EC in September 2002 with Act No. 428/2002 Coll., the Data Protection Act, as amended. In order to solve some application problems of Act No. 428/2002 Coll. resulting from the non-uniform interpretation of the definitions under this Act, the new Act No. 122/2013 Coll., the Data Protection Act ('DPA'), substituting Act No. 428/2002 Coll., has been adopted and is effective as of 1 July 2013 which has been further amended by the Act No. 84/2014 Coll. that is effective as of 15 April 2014.

DEFINITIONS

Definition of personal data

Personal data shall, for the purposes of the DPA, mean any information relating to an identified or identifiable natural person, either directly or indirectly, in particular by reference to an identifier of general application or by reference to one or more factors specific to his/her physical, physiological, psychic, mental, economic, cultural or social identity.

Definition of sensitive personal data

The DPA does not provide for a definition of sensitive personal data. However, one of the provisions of the DPA namely ‘Special categories of data’ refers, inter alia, to personal data related to race, ethnic origin, political opinions, religious belief, as well as data related to the breach of provisions of criminal or administrative law, biometrical data, or data related to the mental status of the data subject.

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Office of the Slovak Republic (‘Office’) is: Úrad na ochranu osobných údajov Slovenskej republiky (Official Slovak Name)

Hraniná 12
820 07, Bratislava 27
Slovak Republic

The Office is responsible for overseeing the DPA in Slovakia.

REGISTRATION

The obligation to register the information system with the Office was replaced with the obligation of the data controller to notify the information systems under the conditions set out in DPA to the Office.

The obligation to notify shall apply to all information systems, in which personal data are processed by fully or partially automated...
means of processing.

The information system needs to be notified before starting with the processing of the data contained therein. Notification may be carried out electronically as well as in the written form, whereas such notification is free of charge. The Office will assign an identification number to the pertinent information system, as well as issue a certificate of the fulfilment of the notification obligation to notify on the controller’s request.

Despite the above, special registration shall remain applicable to the information systems that are stipulated in the DPA, inter alia, those that contain special categories of data or data processed without the data subject’s consent, which is to be transferred to third countries that do not guarantee an adequate level of data protection. The Office will verify whether the data processing could infringe the rights and freedoms of data subjects and decide, within 60 days from the day of its receipt, whether or not it will permit the data processing. The said period may be prolonged by the Office, however in any case for a maximum duration of 6 months. If the Office assesses the data processing in the information system as a risk, it shall not carry out the special registration of the processing for the respective purpose. The Office will carry out the special registration for a fee of EUR 50.

DATA PROTECTION OFFICERS

The data controller is responsible for the internal supervision of protection of personal data processed pursuant to the DPA. The data controller may nominate in writing one or more data protection officers for supervising the observation of the DPA provisions in his/her/its company if he/she/it processes the personal data through authorised persons. The Office must be notified of this fact in writing by the data controller without undue delay, but no later than 30 days from such nomination.

Data protection officers may supervise the observation of the DPA provisions on the basis of his/her nomination only following the successful completion of the professional examination at the Office. The particularities of this examination are stipulated in Decree of the Office No. 165/2013 Coll.

COLLECTION & PROCESSING

Under the DPA, the data controller who intends to process personal data of the data subject must inform the data subject before obtaining the data, and notify him/her in advance of the following:

- identification data of the data controller and his/her/its representative (if appointed)
- identification data of the data processor, provided that the data controller processes personal data from the data subject through the data processor
- the purpose of the personal data processing
- list (or extent) of personal data, and
- additional information in the extent necessary for safeguarding the rights and legitimate interests of the data subject with regard to all circumstances of the processing of personal data, the particulars of which are provided in the DPA.

Personal data may be processed only by the data controller or data processor. The data processor may process personal data only to the extent and under the conditions agreed with the data controller in a written contract.

The DPA lists basic obligations of the data controller mentioned below. The data controller must, inter alia:

- determine unambiguously and specifically the purpose of data processing before starting the data processing; the purpose of data processing must be clear and it cannot be contrary to the Constitution of the Slovak Republic, constitutional laws, laws and international treaties binding for the Slovak Republic
- determine the conditions of the data processing in a manner so that the rights of the data subject under the DPA are not restricted
• process only accurate, complete and, where necessary, updated personal data in respect of the purpose of its processing

• destroy the personal data when the purpose of processing is terminated, and

• process personal data in accordance with public morals and act in a manner not contrary to the DPA.

Personal data may only be processed upon the consent of the data subject, unless provided otherwise for by the DPA. The consent of the data subject is not required for instance in cases when the purpose of the data processing, data subjects and the list (or extent) of the personal data is stipulated by a directly enforceable legally binding Act of the EU, an international treaty binding for the Slovak Republic, the DPA or other particular Acts. Under the DPA, the processing of special categories of data (ie sensitive information) is allowed only upon the written or other reliably verifiable consent of the data subject and following the specific conditions set forth in the DPA.

TRANSFER

Transfer to third parties within the territory of the Slovak Republic

The personal data of the data subject may be transferred from the information system to another natural person or legal entity only upon obtaining the written confirmation of the data subject’s consent, if the DPA requires such consent; the person providing data in such manner may replace this written confirmation by a written declaration of the data controller stating that the data subjects gave their consent, provided that the data controller is able to prove that the written consent of the data subjects was given.

Transfer to non-EU member states (ie third countries) that offer an adequate level of data protection

If the third country guarantees an adequate level of data protection, the data may be transferred to this country if the data controller informed the data subject about the facts required to obtain the data subject’s data (ie the information mentioned above in relation to data collecting by the data controller). Under the DPA, the data transfer to a country that guarantees an adequate level of protection is also allowed in cases when a notification/information to the data subject is not required.

Transfer to third countries that do not offer an adequate level of data protection

If the third country does not guarantee an adequate level of protection, the transfer of data is possible if the data controller adopts appropriate guarantees to protect:

• the privacy and fundamental rights and freedoms of natural persons (data subjects), and
• the enforcement of such rights. Such guarantees result either from standard contractual clauses under special regulations or from binding internal rules of the data controller, which were approved by the supervisory authority in the field of data protection with its seat in an EU or EEA Member State.

If, in the contract on transfer of personal data to the third country which does not offer an adequate level of protection, the data controller uses the contractual clauses which are different from the contractual clauses referred to above and/or are obviously non-compliant with them, the data controller is obliged to obtain the consent of the Office for such transfer in advance.

Otherwise, the transfer of data to a third country that does not offer an adequate level of protection is possible only if the conditions mentioned below are fulfilled:

• before the actual transfer, the data subject gave a written or other reliably verifiable consent to the transfer, while knowing that the country of final destination does not ensure an adequate level of protection

• the transfer is necessary for the execution of a contract between the data subject and the data controller or for pre contractual measures or in negotiations regarding the amendments to the contract which are initiated upon the request of the data subject
- it is necessary for entering into, or the execution of, a contract concluded by the data controller in the interest of the data subject with another entity

- it is necessary or desired under the respective law for securing an important public interest or for proving, filing or defending a legal claim resulting from an international treaty binding for the Slovak Republic or resulting from the laws

- it is necessary for the protection of vital interests of the data subject, or

- it concerns the personal data, which constitutes a part of the lists, registers or files and are kept and publicly accessible pursuant to special legislation or is available, under this legislation, to persons who prove that they are legally entitled and fulfil the conditions prescribed by law for making the data available.

**Transfer to the US**

For the transfer of data to the United States, compliance with the US/EU Safe Harbor principles no longer satisfies the requirements of the DPA provisions on data transfer. Therefore, on 12 July 2016, the EU Commission adopted the decision on the EU-US Privacy Shield. This new arrangement complies with the requirements stipulated by the European Court of Justice in its judgement issued on 6 October 2015 in the case of Schrems (C-362/14).

The Privacy Shield allows for the personal data to be transferred from the EU to a US company, if such a US company signs up to the Privacy Shield framework with the US Department of Commerce. The obligations applying to the US companies under the Privacy Shield are contained in the Privacy Principles. The details of all the companies taking part in the Privacy Shield may be found in the Privacy Shield List, which is available on the website of the US Department of Commerce (https://www.privacyshield.gov/welcome).

If the US company is not a member of the Privacy Shield, the mechanisms enabling the data transfer to the countries which do not guarantee an adequate level of data protection, which are described above, may be used.

**SECURITY**

The data controller is responsible for the security of personal data by protecting it against damage, destruction, loss, alteration, unauthorised access and making available, providing or publishing, as well as against any other unauthorised forms of processing. For this purpose, the data controller must take reasonable technical, organisational and personal measures which correspond to the manner of processing data.

The data controller is required to prepare a security project, for certain information systems under the conditions stipulated in the DPA. Particularities of the security requirements are in detail stipulated by Decree of the Office No. 164/2013 Coll.

The data controller may nominate in writing one or more data protection officers for supervising the observation of the DPA provisions in his company if he/she/it processes the personal data through authorised persons. The data controller is required to instruct the authorised persons about the rights and obligations stipulated in the DPA before the first operation with the personal data is carried out. The data controller must establish and maintain confidentiality of the processed data even after the termination of its processing.

**BREACH NOTIFICATION**

Under the DPA, there is no mandatory requirement to report data security breaches or losses to the Office. However, this does not affect the ability of other public authorities to report data security infringements or losses to the Office if they suspect that such an event might have occurred.

**ENFORCEMENT**

The Office is responsible for the enforcement of the DPA. Upon a complaint from a data subject or another person or a report from public authorities, the Office shall commence administrative proceedings to ascertain possible breaches of obligations or conditions stipulated by the DPA and eventually shall impose a fine for these breaches. The Office may issue decisions to provide temporary relief for the data subject or to ensure due rectification depending on the nature of the breach.
The Office shall impose fines for breaches of the DPA between EUR 150 to EUR 200,000. The Office may publish a notice containing the identity of the data controller or data processor that breached the provisions of the DPA and the final decision of the Office regarding such breach, including its descriptions, and merits of the case. The Office shall also impose disciplinary fines on the data controller or the data processor in instances stipulated by the DPA.

**ELECTRONIC MARKETING**

Electronic marketing shall be governed by Act No. 351/2011 Coll. on Electronic Communications, as amended (‘ECA’).

Under the ECA, processing of the traffic data of a subscriber or user for the purposes of marketing services or purposes of ensuring the value added services by any public network or service providers is possible solely with the prior consent of the subscriber or the user.

Prior to obtaining the consent, the public network or service providers are obliged to inform the subscriber or user on:

- the type of the traffic data processed
- the purpose of the traffic data processing, and
- the duration of the data processing.

For the purposes of direct marketing, the call or use of automatic calls and communications systems without human intervention, facsimile machines, e-mail, including SMS messages to the subscriber or user, who is a natural person, is allowed solely with his/her prior consent. Such consent shall be proved. Users or subscribers are entitled to withdraw such consent at any time.

The prior consent of the recipient of a marketing e-mail shall not be required in the case of direct marketing of own similar products and services of a person, that has obtained electronic contact information of the recipient from the previous sale of its own product and/or service to such recipient and in line with the provisions of the ECA. The recipient of an e-mail shall be entitled to refuse at anytime, by simple means and free of charge such use of electronic contact information at the time of its collection and on the occasion of each message delivered in the case the recipient has not already refused such use.

Both,

- sending e-mails for the purposes of direct marketing without the determination of a valid address to which the recipient may send a request that he/she is no longer willing to receive such communication, and
- encouragement to visit a website in contradiction with a special regulation, shall be prohibited.

**ONLINE PRIVACY**

As regards the protection of privacy and protection of personal data processed in the electronic communications sector, the provisions of the ECA shall apply. The ECA implemented Directive 2002/58/EC (as amended by Directive 2009/136/EC).

Under the ECA, the public network or service provider is obliged to ensure technically and organisationally the confidentiality of the communications and related traffic data, which are conveyed by means of its public network and public services. In particular recording, listening, or storage of data (or other kinds of an interception or a surveillance of communications and data related thereto) by persons other than users, or without the consent of the concerned users, shall be prohibited. However, this does not prohibit the technical storage of data, which is necessary for the conveyance of communications. However, the principle of confidentiality shall still apply.

Further to this, the network or service provider (‘undertaking company’) shall not be held liable for the protection of the conveyed information if such information can be directly listened to or obtained at the location of the broadcasting and/or reception.

However, this ban does not apply to temporary recording and storing of messages and 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.

Under the ECA, each person that stores or gains access to the information stored in the terminal equipment of a user must be authorised for such processing by the concerned user whose consent must be based upon exact and complete information regarding the purpose of such processing of the data. In this regard, also the use of the respective setting of the web browser or other computer programme is considered (implied) consent.

Traffic Data

Traffic Data can only be processed for the purpose of the conveyance of a communication on an electronic communications network or for the invoicing thereof. The Traffic Data related to subscribers or users may not be stored without the consent of the person concerned 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 ECA.

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 or the court in the case of a dispute between undertaking companies or between an undertaking company and a subscriber. The scope of the stored Traffic Data must be limited to the minimum necessary.

Location Data

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 user consent, and in the scope and time necessary for the provision of the value added service. 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 purpose and duration, 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.

Following the Judgment of the Court of Justice of the European Union on 8 April 2014 in the joined cases of Digital Rights Ireland (C-293/12) and Kärntner Landesregierung (C-594/12) which cancelled so called "data retention" Directive 2006/24/EC, Constitutional Court of Slovak Republic on 29 April 2015 issued a Judgement (PL. ÚS 10/2014-78) (“Judgement”) upon which the Constitutional Court proclaimed the certain provisions of the ECA to be non-compliant with the provisions of the Constitution of Slovak Republic, provisions of the Charter of Fundamental Rights and Freedoms and with the provisions of the Convention for the Protection of Human Rights and Fundamental Freedoms. Upon the Judgment, the obligation of the telecommunications operators to retain the Traffic Data and Location Data about the electronic communication of all citizens for the prescribed period (6/12 months) was abolished and removed from ECA.
DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation’s level of data protection maturity.
**SLOVENIA**

_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 new Slovenian Data Protection Act (ZVOP-2) that will implement certain aspects of the GDPR has still not been adopted. It entered the legislative procedure in April 2018 (latest available version), but the Slovenian parliament was dissolved due to a general election so all legislative procedures were stopped. It is unclear what the final outcome will be or when the final act will be adopted (expected in autumn 2018). A new government has not been formed yet as no party is able to produce the needed majority, therefore a re-election is also a possible scenario.

The current draft mostly follows the GDPR and only amends a few aspects, mostly of a systemic and procedural nature and adds some provisions in areas where GDPR allows to do so. We have to note that the academia and other stakeholders have voiced their concerns regarding the suitability of the current draft. Based on this, it is expected that the draft will undergo further major revisions. Furthermore, the new government may pursue a different policy regarding data protection which could cause further revisions.

_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.

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 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. 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 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.

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, a change which is currently forecast for Spring 2019. 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 98/04 et seq.), the Electronic Commerce Market Act (Zakon o elektronskem poslovanju na trgu, Official Gazette 19/15), the Electronic Communications Act (Zakon o elektronskih komunikacijah, Official Gazette no. 109/12 et seq.) and the Personal Data Protection Act.

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-1) provides rules on the usage of cookies and similar technology for data storage.

Pursuant to ZEKom-1 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

**DATA PRIVACY TOOL**

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

LAW

The right to privacy is recognised and protected as a fundamental human right in the Bill of Rights of the Constitution of the Republic of South Africa.

The Protection of Personal Information Act ("POPI"), which introduces an overarching regulatory framework for the processing of personal information, was signed into law on 19 November 2013. POPI intends to promote the protection of personal information processed by public and private bodies and introduces minimum requirements for the processing of personal information. The Act also provides for the establishment of an Information Regulator ("Information Regulator"), a body tasked with monitoring compliance with, and enforcement of, the provisions of POPI.

To date, only certain sections of POPI (including the definitions section and the provisions dealing with the establishment of the office of the Information Regulator) have come into effect. The remaining sections will come into effect upon proclamation of commencement by the President of the Republic of South Africa. The Information Regulator has indicated that it hopes to be fully operational by the end of 2018, after which the process to bring the remaining sections of POPI into effect will begin.

DEFINITIONS

Definition of personal data

POPI applies (subject to certain exclusions discussed below) to the processing of 'personal information' which is defined as information relating to an identifiable, living, natural person, and where applicable, an identifiable juristic person, including:

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin; colour, 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, e-mail 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.

POPI does not apply to the processing of 'personal information':

Last modified 24 January 2018
• in the course of a purely personal or household activity;
• in a way in which it 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, defence or public safety, or the prevention, investigation or proof of offences;
• 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;
• for bona fide literary or artistic expression;
• by Cabinet and its committees, the Executive Council of a province and a Municipal Council of a municipality (this option may be deleted in the final version of the PPI Act when it is promulgated);
• for purposes relating to the judicial functions of a court referred to in section 166 of the Constitution;
• 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; and
• under circumstances that have been exempted from the application of the information protection principles by the Information Regulator in certain circumstances.

Definition of sensitive personal data

Personal information concerning religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information or criminal behaviour (to the extent that such information relates to the alleged commission of an offence or any proceedings in respect of any offence allegedly committed, or the disposal of such proceedings) is defined as "special personal information".

Subject to certain prescribed exceptions, the processing of special personal information is prohibited.

NATIONAL DATA PROTECTION AUTHORITY

The first members of the Information Regulator have been appointed, with effect from 1 December 2016. It is envisaged that the draft regulations will be submitted to Parliament for tabling in February 2018. The anticipated date of publication of the final regulations is April 2018.

The powers, duties and functions of the office of the Information Regulator include providing education regarding the protection and processing of personal information; monitoring and enforcing compliance with the provisions of POPI; 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 POPI as "information officers") must be registered with the Information Regulator prior to taking up their duties in terms of the Act.

No registration is required to process personal information, however, prior authorisation must be obtained from the Information Regulator before processing of personal information in certain circumstances, prescribed in section 57 of POPI.

DATA PROTECTION OFFICERS

In terms of POPI the duties and responsibilities of a body’s data protection officer (information officer) include encouraging and ensuring compliance, by the body, with POPI; dealing with any requests made to that body in terms of POPI; and working with the Information Regulator in relation to investigations by the Information Regulator in relation to that body.

COLLECTION & PROCESSING

"Processing" of information is defined in POPI as any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:
• the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
• dissemination by means of transmission, distribution or making available in any other form; or
• merging, linking, as well as blocking, degradation, erasure or destruction of Information.

POPI prescribes eight conditions for the lawful processing (which includes collection) of personal information namely accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation.

Various requirements are listed under each condition. These include that:
• the processing is performed in a reasonable manner that does not infringe the data subject’s privacy and is adequate, relevant and not excessive;
• all necessary notifications and consents (as prescribed) are obtained;
• personal information is collected for a specific, explicitly defined and lawful purpose and, except in certain prescribed exceptions, is collected directly from the data subject;
• appropriate steps are taken to secure the integrity and confidentiality of personal information; and
• data subjects may request that their personal data be corrected or deleted.

TRANSFER

POPI 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 which has been received from outside South Africa.

Receiving personal information from other countries

The requirements for the processing of personal information prescribed in POPI 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 POPI, an
  ▪ includes provisions that are substantially similar to those contained in POPI 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; and
• 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 POPI 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:
• 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 POPI, where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised 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 offences 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 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:

• 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 unauthorised person who may have accessed or acquired the personal information.

The Information Regulator may direct a responsible party to publicise, 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.

ENFORCEMENT

Any person may submit a complaint to the Information Regulator alleging non-compliance with POPI. The Information Regulator may also initiate and 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 may issue an enforcement notice prescribing action to be taken by the responsible party to remedy the situation.
A responsible part who fails to comply with an enforcement notice is guilty of an offence 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 which may be imposed in terms of both sections 107 and 109 is ZAR10 million although this may change once the regulations are promulgated.

Section 99 also makes provision for a civil action for damages resulting from non-compliance with POPI.

**ELECTRONIC MARKETING**

The Electronic Communications and Transactions Act and the Consumer Protection Act empowers consumers to restrict unwanted direct marketing.

In terms of POPI, the processing of a data subject’s personal information for the purposes of direct marketing is prohibited unless the data subject has given its consent, or the email recipient is a customer of the responsible party. When sending emails to a data subject who is a customer, the responsible party must have obtained the details of the data subject through a sale of a product or service, the marketing should relate to its own similar products or services and the data subject must have been given a reasonable opportunity to object to the use of its personal information for marketing when such information was collected.

**ONLINE PRIVACY**

There are no sections of POPI which regulate privacy in relation to cookies and location data. These issues may be dealt with in subsequently regulations or codes of conduct to be issued by the Information Regulator.

---

**KEY CONTACTS**

**DLA Piper**

**Janine Simpson**

Director

DLA Piper

T 0027 (0) 11 282 0797

janine.simpson@dlapiper.com

---

**DATA PRIVACY TOOL**

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

In the past, South Korea did not have a comprehensive law governing data privacy. However, a law relating to protection of personal information (Personal Information Protection Act, 'PIPA') was enacted and became effective as of 30 September 2011.

Moreover, there is sector specific legislation such as:

- the Act on Promotion of Information and Communication Network Utilisation and Information Protection ('IT Network Act') which regulates the collection and use of personal information by IT Service Providers, defined as telecommunications business operators under Article 2.8 of the Telecommunications Business Act; and other persons who provide information or intermediate the provision of information for profit by utilising services rendered by a telecommunications business operator.

- the Use and Protection of Credit Information Act ('UPCIA') which regulates the use and disclosure of Personal Credit Information, defined as credit information which is necessary to determine the credit rating, credit transaction capacity, etc. of an individual person. The UPCIA primarily applies to Credit Information Providers/Users, defined under Article 2.7 of the UPCIA as a person (entity) prescribed by Presidential Decree thereof who provides any third party with credit information obtained or produced in relation to his/her own business for purposes of commercial transactions, such as financial transactions with customers, or who has been continuously supplied with credit information from any third party to use such information for his/her own business, and

- the Act on Real Name Financial Transactions and Guarantee of Secrecy ('ARNFTGS') which applies to information obtained by financial or financial services institutions.

Under PIPA, except as otherwise provided for in any other Act, the protection of personal information shall be governed by the provisions of PIPA.

DEFINITIONS

Definition of personal data

Under PIPA, information pertaining to a living individual, which contains information identifying a specific person with a name, a national identification number, images, or other similar information (including information that does not, by itself, make it possible to identify a specific person but that which enables the recipient of the information to easily identify such person if combined with other information).

Under the IT Network Act, information pertaining to a living individual, which contains information identifying a specific person with a name, a national identification number, or similar in a form of code, letter, voice, sound, image, or any other form (including information that does not, by itself, make it possible to identify a specific person but that enables such person to be identified...
The relevant Korean authorities’ understanding is that the construction of Personal Data under PIPA and that under IT Network Act are the same in spite of subtle differences in definition wordings.

**Definition of sensitive personal data**

Under PIPA, Sensitive Personal Data is defined as Personal Data consisting of information relating to a living individual’s:

- thoughts or creed
- history regarding membership in a political party or labour union
- political views
- health care and sexual life, and
- other Personal Data stipulated under the Enforcement Decree (the Presidential Decree) which is anticipated to otherwise intrude seriously upon the privacy of the person.

The Enforcement Decree of PIPA includes genetic information and criminal record as Sensitive Personal Data. The IT Network Act also has a similar definition.

**NATIONAL DATA PROTECTION AUTHORITY**

The Ministry of the Interior ("MOI") is in charge of the execution of PIPA. The Korea Communications Commission ("KCC") is in charge of the execution of the IT Network Act.

**REGISTRATION**

Under PIPA, a public institution which manages a Personal Data file (collection of Personal Data) shall register the following with the MOI:

- name of the Personal Data file
- basis and purpose of operation of the Personal Data file
- items of Personal Data which are recorded in the Personal Data file
- the method to process Personal Data
- period to retain Personal Data
- person who receives Personal Data generally or repeatedly, and
- other matters prescribed by Presidential Decree. A ‘public institution’ in this context refers to any government agency or institution.

The Presidential Decree of PIPA stipulates that the followings also shall be registered with the MOI:

- the name of the institution which operates the Personal Data file
- the number of subjects of the Personal Data included in the Personal Data file
- the department of the institution in charge of Personal Data processing
• the department of the institution handling the Personal Data subjects’ request for inspection of Personal Data, and

• the scope of Personal Data inspection of which can be restricted or rejected and the grounds therefore.

Only ‘public institutions’ are required to register with the MOI.

DATA PROTECTION OFFICERS

Under PIPA, every Data Handler (which means any person, any government entity, company, individual or other person that, directly or through a third party, handles Personal Data in order to manage Personal Data files for work purposes) must designate a data protection officer.

Under the IT Network Act, every IT Service Provider must designate a director or chief officer of the department in charge of handling Personal Data as a data protection officer. Pursuant to Presidential Decree of the IT Network Act where, an IT Service Provider has less than 5 employees, the owner or representative director shall be the person in charge.

There are no nationality or residency requirements for the data protection officer. In the event that a data protection officer is not designated, the Data Handler may be subject to a maximum administrative fine of KRW 10 million under the PIPA or KRW 20 million under the IT Network Act.

COLLECTION & PROCESSING

If a Data Handler under PIPA or an IT Service Provider under the IT Network Act intends to collect Personal Data from the data subject or IT service user, it must:

• first notify the data subject or IT service user of the vital information stipulated under the law, and

• obtain the data subject’s or IT service user’s prior consent to such collection other than some exceptional cases stipulated under the law.

If a Data Handler under PIPA intends to collect Sensitive Personal Information, the consent must be separately obtained.

Under the amended IT Network Act, which became effective as of 18 August 2012, an IT Service Provider shall not collect a Resident Registration number (equivalent to Social Security number in the United States), unless:

• the IT Service Provider is designated as an identification institution by the KCC, or

• there exist special provisions under any other laws or Notification of the KCC.

Under the PIPA, prior to obtaining the prerequisite consent for collecting Personal Data from a data subject, a Data Handler must notify the data subject of:

• the purpose of collection and use of Personal Data

• items of Personal Data to be collected

• time period for possession and use of Personal Data, and

• the fact that the data subject has the right to refuse to consent and the consequences of refusing.

Under the IT Network Act, prior to obtaining prerequisite consent for collecting Personal Data from an IT service user, an IT Service Provider must notify the IT service user of:

• the purpose of collection and use of Personal Data

• items of Personal Data to be collected, and
Under the newly amended PIPA, effective as of 7 August 2014, an Data Handler shall not handle a Resident Registration number, unless:

- there exists special provisions requiring or permitting the handling of the Resident Registration number under other laws
- there is clear evidence of some urgent need to handle the data, for the sake of the safety or property of the data subject or of a third party, or
- the handling of the Resident Registration number is unavoidable and there exist special provisions under ordinance of the MOI.

When a certain business transfer occurs, the Data Handler or IT service provider must provide its data subjects or IT service users a chance to opt out by providing a notice, including items of:

- the expected occurrence of Personal Data transfers
- the contact information of the recipient of the Personal Data, including the name, address, telephone number and other contact details of the recipient, and
- the means and process by which the data subject or IT service user may refuse to consent to the transfer of Personal Data.

If the data subject or IT service user is under 14, the consent of his/her legal guardian must be obtained.

As a general rule, a Data Handler under PIPA or an IT Service Provider under the IT Network Act may not handle Personal Data without obtaining the prior consent of the data subject or IT service user, beyond the scope necessary for the achievement of the Purpose of Use. This general rule also applies where a Data Handler or IT Service Provider acquires Personal Data as a result of a merger or acquisition.

Exceptions to the general rule above apply in the following cases under PIPA:

- where there exist special provisions in any Act or it is inevitable to fulfil an obligation imposed by or under any Act and subordinate statute
- where it is inevitable for a public institution to perform its affairs provided for in any Act and subordinate statute
- where it is inevitably necessary for entering into and performing a contract with a subject of Personal Data
- where it is deemed obviously necessary for the physical safety and property interests of a subject of Personal Data or a third person when the subject of Personal Data or his/her legal representative cannot give prior consent because he/she is unable to express his/her intention or by reason of his/her unidentified address, and
- where it is necessary for a Data Handler to realise his/her legitimate interests and this obviously takes precedence over the rights of a subject of Personal Data. In such cases, this shall be limited to cases where such data is substantially relevant to a Data Handler’s legitimate interests and reasonable scope is not exceeded.

Exceptions to the general rule above apply in the following cases under the IT Network Act:

- if the Personal Data is necessary in performing the contract for provision of IT services, but it is obviously difficult to get consent in an ordinary way due to any economic or technical reason.
- if it is necessary in settling the payment for charges on the IT services rendered, and
if a specific provision exists in this Act or any other Act.

Under the ARNFTGS, financial institutions must obtain written consent for the disclosure of an individual’s information relating to his/her financial transactions.

**TRANSFER**

As a general rule, a Data Handler or an IT Service Provider may not provide Personal Data to a third party without obtaining the prior opt in consent of the data subject or IT service user.

Exceptions to the general rule above apply in the following cases under PIPA:

- where there exist 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, and
- where it is deemed obviously necessary for the physical safety and property interests of a subject of Personal Data or a third person when the subject of Personal Data or his/her legal representative cannot give prior consent because he/she is unable to express his/her intention or by reason of his/her unidentified address, etc.

Exceptions to the general rule above apply under the IT Network Act if a specific provision exists in this Act or any other act otherwise.

Under PIPA, a Data Handler must obtain consent after it notifies the data subject of:

- the person (entity) to whom the Personal Data is furnished
- purpose of use of the Personal Data by the person (entity)
- types of Personal Data furnished
- period of time during which the person (entity) will possess and use the Personal Data, and
- the fact that the data subject has the right to refuse to consent and the consequences of refusing.

Under the IT Network Act, an IT Service Provider must notify the IT service user of:

- the person (entity) to whom the Personal Data is furnished
- purpose of use of the Personal Data by the person (entity)
- types of Personal Data furnished, and
- period of time during which the person (entity) will possess and use the Personal Data, and then obtain consent from the IT service user.

The UPCIA stipulates that prior to obtaining prerequisite consent for providing personal credit information to any other person, a Credit Information Provider/User must notify the credit information subject of:

- the person (entity) to whom the credit information will be furnished
- the purpose of use of the Personal Credit Information by the person (entity)
- the types of Personal Credit Information to be furnished, and
• the period of time during which the person (entity) will possess and use the Personal Credit Information.

Exceptions to the general rule above apply in the following cases under the UPCIA:

• where a Credit Information Company as defined under Article 2.5 of the UPCIA provides such information for the purpose of performing central management and utilisation thereof with another Credit Information Company or Credit Information Collection Agency as defined under Article 2.6 of the UPCIA

• where such provision is required to perform a contract, and to entrust the processing of credit information under Article 17.2 of the UPCIA

• where the relevant Personal Credit Information is provided as part of rights and obligations that are transferred by way of business transfer, division, merger, etc.

• where Personal Credit Information is provided for a person who uses the information for purposes prescribed by Presidential Decree, including claims collection (applicable only to the credit which is an object of collection), license and authorisation, determination of a company’s credit worthiness, and transfer of securities

• where Personal Credit Information is provided in accordance with a court order for submission thereof or a warrant issued by a judicial officer

• where such information is provided upon the request of a prosecutor or judicial police officer, in the event of occurrence of an emergency where a victim’s life is in danger or he/she is expected to suffer bodily injury, etc., so that no time is available to issue a judicial warrant

• where such information is provided as the head of a competent government office requests, in writing, for the purpose of inquiry and examination in accordance with any laws pertaining to taxes or demands the taxation data required to be provided in accordance with such laws pertaining to taxes

• where Personal Credit Information held by a financial institution is provided to a foreign financial supervisory body in accordance with international conventions, etc.

• where information by which the credit worthiness of related persons, such as a violator of credit order prescribed by Presidential Decree, and an oligopolistic stockholder and the largest investor of an enterprise, can be determined, is provided; and

• where such information is otherwise provided in accordance with other laws.

Under the ARNFTGS, financial institutions must obtain written consent for the transfer of an individual’s information relating to his/her financial transactions to a third party.

Under PIPA, when processing Personal Data acquired indirectly by way of a third party transfer, transferees who meet a certain threshold as provided by the Presidential Decree will be obligated to notify the data subject of (i) the third party source (transferor) from which the Personal Data was acquired, (ii) the intended use of the received Personal Data, and (iii) the fact that the data subject has the right to request for suspension from processing Personal Data.

SECURITY

Under PIPA and IT Network Act, every Data Handler or IT Service Provider must, when it handles Personal Data or Sensitive Personal Data of a data subject or IT service user, take the following technical and administrative measures in accordance with the guidelines prescribed by Presidential Decree to prevent loss, theft, leakage, alteration, or destruction of Personal Data:

• establishment and implementation of an internal control plan for handling Personal Data 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 Data

• measures for preventing fabrication and alteration of access records

• measures for security including encryption technology and other methods for safe storage and transmission of Personal Data

• 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 Data.

**BREACH NOTIFICATION**

Under PIPA, if a breach of Personal Data occurs the Data Handler must notify the data subjects without delay of the details and circumstances, and the remedial steps planned. If the number of affected data subjects exceeds 10,000, the Data Handler shall immediately report the notification to data subjects and the result of measures taken to MOI, KISA or the National Information Security Agency (‘NIA’).

Under the IT Network Act, an IT Service Provider must, if it discovers an occurrence of intrusion:

- report it to the KCC or the Korea Internet & Security Agency (KISA) within twenty four (24) hours of knowledge of the intrusion, and

- analyse causes of intrusion and prevent damage from being spread, whenever an intrusion occurs.

The KCC may, if deemed necessary for analysing causes of an intrusion, order an IT Service Provider to preserve relevant data, such as access records of the relevant information and communications network.

Under the newly amended IT Network Act, which became effective as of 29 November 2014, if a loss, theft or leakage of Personal Data occurs, the IT Service Provider must notify the IT Service user immediately and report to the KCC within twenty four (24) hours of the details and circumstances, and the remedial steps planned.

**ENFORCEMENT**

The competent authorities may request reports on the handling of Personal Data, and also may issue recommendations or orders if a Data Handler or IT Service Provider violates PIPA or the IT Network Act. Non compliance with a request or violation of an order can result in fines, imprisonment, or both.

For example, MOI, the supervising authority for Data Handlers, can issue a corrective order in response to any breach of an obligation not to provide Personal Data 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, MOI may take an incremental approach and instruct, advise and make recommendations to the Data Handler.

Under the IT Network Act, an IT Service Provider who collected Personal Data without consent of the relevant user shall be subject to the penalty of imprisonment for not more than 5 years or a fine not exceeding KRW 50 million.

Under the UPCIA, a Credit Information Provider/User who has provided Personal Credit Information without consent of the relevant credit information subject shall be subject to the penalty of imprisonment of up to 5 years or a fine not exceeding KRW 50 million.

Under the ARNFTGS, a person who discloses information or data concerning financial transactions shall be punished by imprisonment not exceeding 5 years or by a fine not exceeding KRW 30 million.

**Punitive damages**
In the event that a Credit Information Provider/User suffers any damages resulting from the Data Handler’s conduct, the Credit Information Provider/User may bring a claim against the Data Handler for such damages. In such cases, a Data Handler may not be discharged from liability unless it can prove that there was no intentional act nor negligence on its part.

As of July 25, 2016, as a result of an amendment to PIPA, in instances Personal Data breaches caused by the Data Handler’s intentional act or negligence, the Data Handler may be liable for three times the damages suffered.

**ELECTRONIC MARKETING**

Under the IT Network Act, anyone who intends to transmit an advertisement by information and communication network must receive the explicit consent of the individual, but if the individual either withdraws consent or does not give consent, then an advertisement with commercial purposes may not be transmitted.

In addition, the transmitter of advertisement information for commercial purposes must disclose the following specifically within the advertisement information:

- 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, log, IP information, etc. are also regulated by the IT Network Act as personal data, which if combined with other information enable the identification of a specific individual person easily. Under the IT Network Act, using cookies (or web beacons) must be done with the opt-out consent of the user and the privacy policy must publicise the matters concerning installation, operation and opt-out process for automated means of collecting personal information, such as cookies, logs and web beacons.

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 (the ‘Location-based Service Provider’) shall report to the KCC. Further, any person (entity) who intends to collect location information and provide
the collected location information to location-based service providers (the ‘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 utilising personal location information provided from 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**

Daniel Lee  
Partner  
T +82 2 6270 8899  
daniel.lee@dlapiper.com

**DATA PRIVACY TOOL**

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

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 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.

It is unclear when the new legislation will be ready.

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.

**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 non-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 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. 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 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.

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, a change which is currently forecast for Spring 2019. 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 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. 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 when 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:

• be clearly marked as such by means of the terms PUBLI or PUBLICIDAD placed inside the subject line

• allow the recipient to opt-out at all times, even by the time of registration, and

• 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.

**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. By the end of April 2013, the AEPD has released Guidance Notes on the use of cookies. 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 new regulation requires data controllers to inform cookies’ recipients (referred to in the LSSI as giving users the ‘actual opportunity’) – including legal entities – of the existence and use of cookies, their scope and how to deactivate them. Actual
opportunity is interpreted by the regulator as a procedure by which the user cannot browse the website, for example, without noticing the invitation to review the above-mentioned information and carrying out an active behaviour (even a simple one like pressing the ESC key) to continue browsing after being presented with the information or the opportunity to review it. A semi-transparent layer on the usual homepage screen is a generally approved mechanism to request the consent (although AEPD has indicated in some reports released in 2014 that a two-step warning approach may work best (first warning on the landing page containing the basics, second one on a separate cookies policy including full details). Certain types of cookies (eg session cookies) are exempt from these restrictions as per the WP29 criteria released during the summer of 2012. The Spanish AEPD has made known to the public, by the way of a resolution, that in some cases the delivery of cookies to the computer of a user based in Spain may trigger the application of Spanish Data Protection Act in full.

On location data, the local position is that it may be acceptable provided that:

- users are informed at all times on whether the location system is active
- users have agreed to be located, and
- users have the option (especially when being off-duty if the location data is used in an employment context) to turn off the system.

**KEY CONTACTS**

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

**DATA PRIVACY TOOL**

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

Last modified 24 May 2018

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 Data Protection Act (2018:218) with its complementary provisions (2018:19) - The act is intended to regulate general aspects where the GDPR allows, e.g. processing of social security numbers and processing of data pertaining to criminal offences. On 19 April 2018 the act was officially adopted by the Swedish parliament and the Data Protection Act ("DPA") will enter into force 25 May 2018. On 19 April 2018 a complementary regulation to the Data Protection Act was presented by the Swedish government, which will complement the Data Protection Act with more detailed provisions regarding e.g. data pertaining to criminal offences. The complementary regulation will as well enter into force 25 May 2018.

In addition to the Swedish DPA, a vast number of sector specific acts has been proposed/adopted in Sweden, for example relating the sectors of healthcare, finance, energy and environment, education, referendums/elections, enterprise, energy and communication and labour market.

On 4 April 2018 in a draft to a proposal to the Council on legislation relating to personal data for scientific purposes, the Swedish government criticized the proposal for a new science data act, meaning that an update of other acts (such as ethical review act) will be enough in order to complement the GDPR. As of now it is therefore uncertain whether such act will be a part of a bill that in the future will be passed to the parliament.
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.

Swedish Data Protection Authority ("Datainspektionen"), Drottninggatan 29 5th Floor, Box 8114 104 20 Stockholm
Tel. +46 8 657 6100
datainspektionen@datainspektionen.se
www.datainspektionen.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
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.

No derogations except that the Swedish Public Access to Information and Secrecy Act (2009:400) shall apply in relation to the confidentiality obligation of a DPO within the public sector, instead of article 37 GDPR. (Chapter 1 article 8 DPA).

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](http://www.dlapiperdataprotection.com)), 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.

- Data concerning personal identity numbers/social security numbers may be processed without consent only when manifestly justified having regard to the purpose of the processing the importance of secure identification or some other substantial reason (chapter 3 section 10 DPA).
- Criminal data (art. 10 GDPR) may be processed by other than public authorities only for the purposes of establishing, exercising or defending legal claims, or to comply with a legal obligation. The Swedish Datainspektionen is entitled to prescribe further derogations to this provision (section 5 complementary provisions).
- Swedish law may prohibit controllers to disclose certain data to the data subjects. This applies to the rights in articles 13-15 in the GDPR (chapter 5 section 1 DPA)
- Article 15 GDPR does not apply to personal data in free text that has not been finalized (only for maximum one year) or to memory notes (chapter 5 section 2 DPA)

**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.

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.

No derogations, except that personal data breaches that fall within the Swedish Security Act (1996:627) shall be reported separately in accordance with provisions of that 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).

In relation to authorities, administrative fines under Swedish DPA (Chapter 6, Section 2) may amount to maximum SEK 5 000 000 (in relation to Article 83.4 GDPR) and SEK 10 000 000 (Article 83.5 & 83.6 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, a change which is currently forecast for Spring 2019. 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 to most electronic marketing activities, given that it is likely that such marketing involves processing of personal data (eg an e-mail address is likely regarded as personal data under the Act). Please note that if the data subject’s e-mail address has not been obtained in the context of a customer relationship or similar, the data subject’s consent is, as a main rule, required for electronic marketing. Moreover, a data subject has a right to at any time oppose (‘opt-out’ of) further processing of his or her personal data for marketing purposes.

ONLINE PRIVACY

Pursuant to the Swedish Electronic Communications Act (as amended by e-Privacy Directive 2009/12/EC), a cookie may be stored on a user’s terminal equipment, only if the user has been given access to information on the purpose of the processing and given his or her consent, ie the user must give his/her prior ‘opt-in’ consent before a cookie is placed on the user’s computer. The government stated in the preparatory works to the Swedish Electronic Communications Act that the implementation of the new e-Privacy Directive should not be regarded as a material change. This has been construed by some that implied consent through browser settings shall be regarded as a valid consent under the Act, provided that sufficient information is given to the user eg in a cookie policy. This is, however, unclear and the Swedish Post and Telecom Authority has not issued any guidance in this regard.

Consent is, however, not required for cookies that are:

- used for the sole purpose of carrying out the transmission of communication over an electronic communications network, or
- necessary for the provision of a service explicitly requested by the user.

Wilful or negligent breach of the Swedish Electronic Communications Act in this regard is sanctioned with fines, provided that the offence is not sanctioned by the Swedish Criminal Code (Sw. brottsbalken). However, if the breach is deemed to be minor, no sanction shall be imposed. To our knowledge there has been no case where a website operator has been fined for breach of the Swedish Electronic Communications Act.
KEY CONTACTS

Johan Sundberg
Advokat/Partner
T +46 70 302 75 62
johan.sundberg@dlapiper.com

Johan Thörn
Senior Associate
T T +46 8 769 79 30
johan.thorn@dlapiper.com

DATA PRIVACY TOOL

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

LAW

The processing of personal data is mainly regulated by the Federal Act on Data Protection of 19 June 1992 (‘DPA’) and its ordinances, ie the Ordinance to the Federal Act on Data Protection (‘DPO’) and the Ordinance on Data Protection Certification (‘ODPC’).

In addition, the processing of personal data is further restricted by provisions in other laws, mainly with regard to the public sector and regulated markets.

It should be noted that the DPA is currently subject to a substantial revision. On 15 September 2017, the Federal Council published the final draft and the dispatch to the Federal Parliament regarding the new DPA. The draft will now be discussed in Parliament. Most likely, it will be passed by Parliament at the end of the Spring session 2018, which will trigger the three-month referendum period. All in all, the revised DPA (and the corresponding ordinance) cannot be expected to enter into force before the Summer of 2018 or even at the beginning of 2019. The revision of the DPA aims to strengthen data protection in general and to align the DPA 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.

DEFINITIONS

Definition of personal data

Personal data means all information relating to an identified or identifiable natural or legal person. It should be noted that data relating to legal entities falls within the scope of Swiss data protection law, as opposed to most EU members’ data protection laws. The ongoing revision proposes to exempt data regarding legal entities from the scope of the DPA, and it seems likely that proposal will be accepted.

Definition of sensitive personal data

Sensitive personal data is defined as data on:

- religious, ideological, political or trade union related views or activities
- health, the intimate sphere or racial origin
- social security measures, and
- administrative or criminal proceedings and sanctions.

‘Personality profiles’ are protected to the same extent under the DPA as sensitive personal data. Personality profiles are
collections of data that allow the appraisal of essential characteristics of the personality of an individual.

**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

The FDPIC supervises federal and private bodies, advises and comments on the legal provisions on data protection and assists federal and cantonal authorities in the field of data protection.

The FDPIC informs the public about his findings and recommendations, and maintains and publishes the register for data files.

**REGISTRATION**

The processing of personal data by private persons does not usually have to be notified or registered, respectively. However, private persons must register their data files before the data files are opened, if:

- they regularly process sensitive personal data or personality profiles, or
- they regularly disclose personal data to third parties,

and if none of the following exemptions applies:

- the data is processed pursuant to a statutory obligation
- the Swiss Federal Council has exempted the particular processing from the registration requirement because it does not prejudice the rights of the data subjects (which the Swiss Federal Council has done in the ODP, inter alia, regarding data files from suppliers or customers, provided they do not contain any sensitive personal data or personality profiles).
- the data controller uses the data exclusively for publication in the edited section of a periodically published medium and does not pass on any data to third parties without informing the data subjects.
- the data is processed by journalists who use the data file exclusively as a personal work aid
- the data controller has designated a data protection officer who independently monitors internal compliance with data protection regulations and maintains a list of the data files, or
- the data controller has acquired a data protection quality mark under a certification procedure and has notified the FDPIC of the result of the evaluation.

**DATA PROTECTION OFFICERS**

There is no requirement under Swiss data protection law to appoint a data protection officer.

However, a data controller can be dispensed from registering its data files if it has designated a data protection officer who:

- carries out his/her duties autonomously and independently
- has a certain level of expertise that is appropriate for the relevant data processing at the company (whereas it is not relevant whether or not the respective expertise was acquired in Switzerland).
must check and audit the processing of personal data within the company

must be in a position to recommend corrective measures when detecting any breaches of applicable data protection rules

must have access to all data files and all data processing within the company as well as to all other information that he/she requires to fulfil his/her duties

must maintain records of all data files controlled by the company and provide this list to the FDPIC or affected data subjects upon request, and

may not carry out any other activities that are incompatible with his/her duties as data protection officer.

The data controller must notify the FDPIC of the appointment of a data protection officer and thereupon such data controller will be listed on the public list of companies exempt from the requirement to register their data files.

COLLECTION & PROCESSING

The following principles apply to the collection and processing of personal data (including data of legal entities):

- personal data may only be processed lawfully, in good faith and according to the principle of proportionality

- the collection of personal data and, in particular, the purpose of its processing must be evident to the data subject

- 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, or provided for by law

- the data 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 below)

- personal data must be protected from unauthorised 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
  - law, and

- sensitive personal data or personality files 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
  - law.

TRANSFER

Personal data may be transferred outside Switzerland if the destination country offers an adequate level of data protection. The FDPIC maintains and publishes a list of such countries. It should be noted that under Swiss data protection law, remote access to data residing in Switzerland from outside of Switzerland is considered as transfer/disclosure abroad.
The FDPIC deems the data protection legislation of all EU and EEA countries to be adequate with regard to personal data of individuals. With regard to personal data of legal entities, only a few EU or EEA countries, such as Austria and Liechtenstein, are deemed to provide an adequate level of data protection.

In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad only if at least one of the following conditions is fulfilled:

- Sufficient safeguards, such as data transfer agreements, or other contractual clauses, ensure an adequate level of protection abroad. Data transfer agreements or other contractual clauses must be notified and submitted for approval to the FDPIC whereas mere information is sufficient if model clauses acknowledged by the FDPIC (such as the EU Standard Contractual Clauses for Controller-to-Controller or Controller-to-Processor Transfers) are used.

- For transfers to the US based on data transfer agreements or other contractual clauses, the following additional two requirements must be complied with according to guidance issued by the FDPIC:
  - data subjects must be informed that their data is being transferred to the US and that there is a possibility that the authorities there may access them; and
  - the contractual parties shall undertake to support affected data subjects to exercise their rights vis-à-vis foreign authorities in any way possible.

- Since 12 April 2017, US companies that process data can be certified under the Swiss-US Privacy Shield regime and thereby make themselves subject to its rules. To do so, they must register on the Department of Commerce (DOC) website www.privacyshield.gov/PrivacyShield/ApplyNow and meet the certification requirements. Accordingly, the FDPIC has amended his list of countries indicating adequate data protection legislation, now listing the US among the countries with adequate legislation if the transferee is certified under the Swiss-US Privacy Shield. According to established practice by the FDPIC, no notification is necessary in case the transferee is certified under the Swiss-US Privacy Shield. It should, however, be noted that certification under the EU-US Privacy Shield does by itself not entail certification for the Swiss-US Privacy Shield.

- 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 be notified to the FDPIC.

- The data subject consents to the particular data export (consent must be given for each individual case, a generic consent is not sufficient).

- The processing is directly connected with the conclusion or performance of a contract with 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 the courts.

- The disclosure is required in order to protect the life or the physical integrity of the data subject, or the data subject has made the personal data publicly accessible and has not expressly prohibited its processing.

**SECURITY**

The data controller and any processor must take adequate technical and organisational measures to protect personal data against unauthorised processing and ensure its confidentiality, availability and integrity. In particular, personal data must be protected against the following risks:

- unauthorised or accidental destruction

- accidental loss

- technical errors
The technical and organisational measures must be appropriate, in particular with regard to the purposes of the data processing, the scope and manner of the data processing, the risks for the data subjects and the current technological standards. The ODP sets out these requirements in more detail.

**BREACH NOTIFICATION**

There is no explicit statutory requirement to notify the FDPIC or the affected data subjects of data security breaches under the DPA. However, depending on the scale and severity of a breach, a notification of the data subjects may be necessary based on the data controller’s and processor’s obligation to ensure data security (to avoid further damage), the principle of good faith or pursuant to contractual obligations.

**ENFORCEMENT**

The FDPIC does not have specific direct powers to enforce the DPA. He may investigate cases on his own initiative or at the request of a third party and may issue recommendations that a specific data processing practice be changed or abandoned. If the FDPIC’s recommendation is not complied with, he may refer the matter to the Swiss Federal Administrative Court for a decision.

Furthermore, the DPA provides for criminal liability and fines of up to CHF 10,000 if a private person intentionally fails to comply with the following obligations under the DPA:

- duty to provide information when collecting sensitive data and personality profiles
- duty to safeguard the data subject’s right to information
- obligation to notify the FDPIC with regard to contractual clauses or binding corporate rules in connection with data transfers abroad
- obligation to register data files, or
- duty to cooperate in an FDPIC investigation.

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 message(s)), the UCA generally requires prior consent by the recipient, ie ‘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-consumer relationships as well as to business-business relationships, ie, mass advertisements sent to individuals and to corporations are subject to the same rules.

Direct marketing by telephone is lawful in Switzerland as long as it is not done in an aggressive way (eg by repeatedly calling the same person). However, the UCA prohibits direct marketing by telephone to people who do not wish to receive commercial communication and have expressed that wish (ie opted-out) by having their entry marked in the telephone books and online telephone registers (eg through an asterisk next to their name).

In addition to the rules of the UCA, the general data protection principles under the DPA also apply with regard to electronic marketing activities, eg 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 collection of personal data under the DPA. 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, eg 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, eg by configuring their web browser to reject cookies.

In addition, the general rules under the DPA apply where cookies collect data related to persons who are identified or identifiable, ie, personal data. The collection of personal data through cookies as well as the purpose of such a collection must be evident to the data subject. The personal data collected may only be processed for the purpose:

- indicated at the time of collection
- that is evident from the circumstances, or
- that is provided for by law.

Where the personal data collected through a cookie is:

- considered sensitive data, eg data regarding religious, ideological, political views or activities, or
- so comprehensive that it forms a personality profile, ie permits an assessment of essential characteristics of the personality of a person

the stricter rules pertaining to the processing of sensitive personal data are applicable.

These stricter rules provide, inter alia, that the data subject must be informed of:

- the identity of the data controller
- the purpose of data processing, and
- the categories of data recipients if the data shall be disclosed to third parties.

Further, in relation to the processing of sensitive personal data implied consent is not sufficient; consent must be given expressly.
KEY CONTACTS

Schellenberg Wittmer Ltd
www.swlegal.ch/

Roland Mathys
Partner / Attorney at Law
T +41 (0)44 215 3662
roland.mathys@swlegal.ch

Christine Beusch-Liggenstorfer
Of Counsel/Attorney at Law
T +41 (0)44 215 5272
christine.beusch@swlegal.ch

Samuel Klaus
Associate / Attorney at Law
T +41 (0)44 215 3695
samuel.klaus@swlegal.ch

Gabor Sebestyen
Associate / Attorney at Law
T +41 (0)44 215 5265
gabor.sebestyen@swlegal.ch

DATA PRIVACY TOOL

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

LAW

The former Computer Processed Personal Data Protection Law (‘CPPL’) was renamed as the Personal Data Protection Law (‘PDPL’) and amended on 26 May 2010. The PDPL became effective on 1 October 2012, except that the provisions relating to sensitive personal data and the notification obligation for personal data indirectly collected before the effectiveness of the PDPL remained ineffective. The government later proposed further amendment to these and other provisions, which passed legislative procedure and became effective on 15th March 2016.

DEFINITIONS

Definition of personal data

According to PDPL, personal data means the name, date of birth, I.D. Card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health checks, criminal records, contact information, financial conditions, social activities and other information which may directly or indirectly be used to identify a living natural person.

Definition of sensitive personal data

According to PDPL, sensitive personal data means the personal data relating to medical records, medical treatments, genetic information, sex life, health checks and criminal records.

NATIONAL DATA PROTECTION AUTHORITY

In Taiwan, there is no single national data protection authority. The various ministries and city/county governments serve as the competent authorities.

REGISTRATION

Unlike the CPPL, there is no need to register with any authorities for the collection, processing, usage and international transfer of personal data under the PDPL.

DATA PROTECTION OFFICERS

There is no requirement in Taiwan for the data controller to appoint a data protection officer. However, if the data controller is a government agency, a specific person should be appointed to be in charge of the security maintenance measures.

COLLECTION & PROCESSING

Under the PDPL, the data controller should not collect or process personal data unless there is specific purpose and should
Data Protection Laws of the World

Taiwan

Comply with one of the following conditions:

- Where collection/processing is explicitly stipulated by law
- Where there is a contract or quasi contract between the data controller and the data subject and there is proper security measures in place
- Where the data subject has him/herself disclosed such data to the publics or where the data has been publicised legally
- Where it is necessary for public interest on statistics or the purpose of academic research conducted by a research institution. The data may not lead to the identification of a certain person after the treatment of the provider or by the disclosure of the collector
- Where consent has been given by the data subject (if the data subject has explicitly informed the data subject of the information as required by the PDPL and the data subject has not expressed his/her rejection and further, provided his/her personal data, the consent will be presumed to have been given. However, the data controller should prove the existence of the relevant facts)
- Where it is necessary to enhance the public interest,
- Where the personal data is obtained from publicly available sources, except that where the vital interest of the data subject requires more protection and the prohibition of the processing or usage of such personal information, or
- Where there is no infringement on the rights of interests of the data subject.

Furthermore, except for the exemptions stipulated in the PDPL (eg if it is explicitly stipulated by law that the provision of such information is not required, or if the data subject is fully aware of the contents of the notice, or if it is not profit-seeking purpose and it is obviously not detrimental to the data subject), the data controller is permitted to collect and process personal data only if the data controller unambiguously informs the data subject of the following information prior to or upon the collection:

- Data controller’s name
- Purpose(s) for collecting personal data
- Categories of personal data
- Period, area, recipients and means of using the data
- The data subject’s rights and the methods by which the data subject may exercise those rights in accordance with the PDPL, and
- Where the the data subject has the right to choose whether or not to provide the data, the consequences of not providing the data.

The information collected should in principle only be used for the purpose notified and not for any other purpose unless falling within any of the exceptional circumstances as set forth in the PDPL (eg, where consent has been given by the data subject, or where it is beneficial to the rights or interests of the data subject).

In addition, the Employment Service Act and its Enforcement Rules require that an employer shall not request a job seeker or an employee to provide his/her privacy information which is unrelated to his/her employment. Such privacy information includes physiological information, psychological information and personal life information. When an employer asks a job seeker or an employee to provide his/her privacy information, the personal interest of the data subject should be respected; the request should not exceed necessary scope of specific purposes based on economic demand or public interest, and should have just and reasonable connection with the specific purposes.
As to sensitive personal data, its collection, processing or usage (including international transfer) is prohibited unless any of the statutory conditions is met, which include the circumstances where written consent of the data subject has been obtained (except that it exceeds the necessary scope of specific purposes, or other laws otherwise provide for, or the consent is contrary to his/her free will), or where the data subject has him/herself disclosed such data to the public or the data has been publicized legally.

TRANSFER

The central competent authority may restrict the international transfer of personal data by the data controller which is not a government agency if:

- where it involves major national interests
- an international treaty or agreement specifies otherwise
- where the country receiving personal data lacks proper regulations that protect personal data and that might harm the rights and interests of the data subject, or
- where the international transfer of personal data is made to a third country through an indirect method in order to evade the provisions of the PDPL.

SECURITY

Data controllers should adopt proper security measures (both technical and organisational) to prevent personal data from being stolen, altered, damaged, destroyed or disclosed.

The central competent authority may request the data controller which is a non-government agency to set up a plan for the security measures of the personal data file or the disposal measures for the personal data after termination of business.

BREACH NOTIFICATION

Where the personal data is stolen, disclosed, altered or infringed in other ways due to the violation of the PDPL, the data controller should notify the data subject after due inquiry.

ENFORCEMENT

Under the PDPL, the competent authority may perform an inspection, if it is necessary for the examination of the security measures of data files, of the disposal measures after termination of business, the limitation of international transfer, or other routine business, or if the PDPL may be violated. Those who perform the inspection may ask the data controller to provide a necessary explanation, take cooperative measures, or provide relevant evidence.

When the competent authority conducts such an inspection, it may seize or duplicate the personal data and files that may be confiscated or may be used as evidence. The owner, holder or keeper of the data or files should surrender them upon request.

In addition, a breach of the PDPL may be subject to criminal sanctions (if for profit-seeking purpose), administrative fines, and civil compensation (collective action is permitted).

ELECTRONIC MARKETING

The PDPL applies to electronic marketing in the same way as to other marketing. Within the necessary scope of specific purposes of data collection, the data controller may use personal data for marketing. However, when the data subject refuses the marketing (a right to ‘opt-out’), the data controller should cease using such personal data for marketing. In addition, when making the first marketing, the data controller should bear the costs to provide the data subject with the means to refuse marketing.

ONLINE PRIVACY
There is no special law or regulation applicable to online privacy. The PDPL applies to online and physical world in the same manner. As a result, online unique issues are not specifically addressed.

**KEY CONTACTS**

Formosa Transnational Attorneys at Law  
www.taiwanlaw.com/

**Chun-yih Cheng**  
Senior Partner  
T +886 2 27557366 Ext 158  
chun-yih.cheng@taiwanlaw.com

**DATA PRIVACY TOOL**

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

LAW

At present, Thailand does not have any general statutory law governing data protection or privacy. However, the Constitution of the Kingdom of Thailand does recognize the protection of privacy rights. In addition, statutory laws in some specific areas (such as telecommunications, banking and financial businesses (Specific Businesses)) as well as other non-business related laws, such as certain provisions under Thai Penal Code and the Child Protection Act B.E. 2543 (2003), do provide a certain level of protection against any unauthorised collection, processing, disclosure and transfer of personal data.

Recently, the draft Personal Information Protection Act (‘Draft’), which has been reviewed by the Council of State, was given to the Committee for House of Representative Coordination to review and analyse if there are any practical issues on applying the law and how the Data Protection Committee should be formed.

The Draft is being reviewed by the Office of the Public Sector Development Commission and will be submitted to the Cabinet for approval later. The current Draft provides protection of personal data by restricting the gathering, using, disclosing and altering of any personal data without the consent of the data owner. The Draft also imposes both criminal penalties and civil liability for any violation of the Draft and calls for the establishment of a Protection of Personal Data Commission to regulate compliance with the Draft.

Notwithstanding the above, at present, no clear indication exists as to when the Draft will be final, or whether it will ultimately be enacted into binding law.

DEFINITIONS

Definition of personal data

According to the Draft, ‘personal data’ means any information or data relating to an identified natural person or that can identify a natural person by reference to the facts, data or any other materials about that natural person.

The information or data may be in the form of documents, files, reports, books, charts, portraits, photos, films, recorded images or sounds that may be kept or stored in computer machines or in any other means that can be used to make the recorded information or data seen. Personal Data shall also include facts about, or behaviours of, a deceased person.

Definition of sensitive personal data

Not available in the present Draft.

NATIONAL DATA PROTECTION AUTHORITY

None at present – see detail in ‘Law’ section above.
REGISTRATION

No registration requirement with respect to the collection or use of personal data exists.

DATA PROTECTION OFFICERS

No requirement exists in Thailand for an organisation to appoint a data protection officer.

COLLECTION & PROCESSING

Statutory laws provide a certain level of protection for the accumulation, retention and release of personal data for Specific Businesses.

For example, a telecommunications operator may collect personal data from customers only for the purpose of its business operation and as permissible by law. The collection of sensitive information, such as physical handicaps or genetics, is strictly prohibited. Operators must also have proper security measures in place to protect customers’ data, including any of their personal data. Any release of personal data, except disclosure for national security purposes, requires the data owner’s consent.

According to the Child Protection Act, the guardian of a child’s safety or a child’s safety protector are forbidden to disclose the name, surname, picture or any information regarding the child and the child’s guardian in a manner which is likely to be detrimental to the reputation, esteem or entitlements of the child. This is also applied mutatis mutandis to a competent official, social worker, psychologist or person having the duty to protect a child’s safety, who has come into the possession of such information as a result of the performance of his or her duties. It is also forbidden for any person to advertise or disseminate by means of the mass media or any other form of information technology the disclosed information in violation of the aforementioned provisions.

If no specific statutory law is applicable then generally, the collection and processing of personal data with the consent (preferably written) of the data owner is permissible.

TRANSFER

Under the Thai Civil and Commercial Code, a person who wilfully, negligently, or unlawfully injures the life, body, health, liberty, property or any right of another person has committed a wrongful act and is required to compensate the victim. Disclosure or transfer of data may be considered a wrongful act if it causes damage to the data owner.

In practice, the prior written consent of the data owner should be obtained before transferring the data to any third person. Disclosure of data without the consent of the data owner is permissible in very limited circumstances (eg pursuant to an order from a government authority or Thai court).

SECURITY

Data controllers in Specific Businesses are required to maintain an appropriate level of security to protect any stored personal data from unauthorised access. Failure to comply with this requirement normally results in both imprisonment and monetary penalties.

Data controllers in non-Specific Businesses are also recommended to implement appropriate security measures to protect personal data from unauthorised access. If unauthorised access causes any damage to the data owner, the data controller may also be liable under the Thai Civil and Commercial Code for committing a wrongful act by failing to prevent the unauthorised access.

BREACH NOTIFICATION

No notification requirement exists with respect to privacy or data protection law.

ENFORCEMENT
No organisation in Thailand is primarily responsible for the enforcement of privacy or data protection law.

**ELECTRONIC MARKETING**

Presently, there is no specific law that prohibits the use of personal data for the purposes of electronic marketing. The availability of option for opt-in and opt-out is just the practice as a norm and not yet the law.

**ONLINE PRIVACY**

At present, there is no provision under the relevant laws and the Draft that specifically prohibits or controls the placing of cookies on users' computers.

Although there are provisions under the Computer Crime Act B.E. 2550 (2007), imposing punishments for certain computer data alterations, the computer cookies or location tracing mechanisms are excluded as they will not cause any of the above alterations to happen to computers. Those below acts are punishable:

- any person who illegally damages, destroys, corrects, changes or amends a third party's computer data, either in whole or in part, shall be subject to imprisonment for no longer than 5 years or a fine of not more than THB 100,000, or both

- any person who illegally commits any act that causes the working of a third party's computer system to be suspended, delayed, hindered or disrupted to the extent that the computer system fails to operate normally shall be subject to imprisonment for no longer than 5 years or a fine of not more than THB 100,000, or both, and

- any person sending computer data or electronic mail to another person and covering up the source of such aforementioned data in a manner that disturbs the other person’s normal operation of their computer system shall be subject to a fine of not more than THB 100,000.

**KEY CONTACTS**

Chadaporn Ruangtoowagoon  
Senior Associate  
T +662 686 8579  
chadaporn.ruangtoowagoon@dlapiper.com

**DATA PRIVACY TOOL**

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

LAW

In Trinidad and Tobago The Data Protection Act, 2011 provides for the protection of personal privacy and information (‘DPA’) processed and collected by public bodies and private organisations.

The DPA was partially proclaimed on the 6th January 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 have come into operation.

No timetable has been set for the proclamation of 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 data (which is referred to in the DPA as ‘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, and

- the fingerprints, DNA, blood type or other biometric characteristics of the individual.
Definition of sensitive personal data

Sensitive Personal Data (which is referred to in the DPA as ‘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, or
- criminal or financial record.

NATIONAL DATA PROTECTION AUTHORITY

The entity responsible for the oversight, interpretation and enforcement of the DPA is the Office of the Information Commissioner. It has broad authority, including to authorise 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. Furthermore, collection is required to be undertaken in accordance with the purpose identified by the organisation collecting, the personal information and other legal requirements.

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 respectively, 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 authorised by law
- the information is collected for the purpose of law enforcement
- the information relates directly to and is necessary for an operating programme or activity of the public body
- the collection of personal information is collected directly from the individual:
  - another method of collection is authorised 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
  - 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 authorisation 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 organisations will 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 with the General Privacy Principles (which are currently in force).

**Sensitive Information**

As to both public bodies and private organisations, Sensitive Personal Information may not be processed 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
- for the purpose of determining access to social services, or
- as otherwise authorised by law.

**TRANSFER**

Section 6(1) of the DPA provides that personal information may be transferred outside of Trinidad and Tobago only if the foreign country requesting the individual’s personal information has safeguards for the regulation of the personal information which are comparable to Trinidad and Tobago’s.

In this regard, the Office of the Information Commissioner is required to publish in the Gazette and at least two newspapers in daily circulation in Trinidad and Tobago a list of countries which have comparable safeguards for personal information as provided by this Act. As of January 6, 2015, this has not yet happened because a Commissioner has yet to be appointed.

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 it must require at a minimum that personal information under the custody or control of a private organisation 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 organisation is to be disclosed to a party residing in another jurisdiction, the organisation 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 organisation shall be responsible for the personal information under its control
- the purpose for which personal information is collected shall be identified by the organisation 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 organisation
The DPA generally requires that personal information be 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 (s.9 (1)).

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.

**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

DATA PRIVACY TOOL

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

LAW

The main piece of legislation covering data protection in Turkey is the Law on the Protection of Personal Data No. 6698 dated 7 April 2016 ("LPPD"). The LPPD is primarily based on EU Directive 95/46/EC.

To date, three Regulations have been enacted in order to implement various aspects of the LPPD:

a. Regulation on the Erasure, Destruction and Anonymizing of Personal Data (published in the Official Gazette dated 28 October 2017 numbered 30224);

b. Regulation on the Working Procedures and Principles of Personal Data Protection Board (published in the Official Gazette dated 16 November 2017 numbered 30242); and

c. Regulation on the Registry of Data Controllers (published in the Official Gazette dated 30 December 2017 numbered 30286).

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 Kiisel Verileri Koruma Kurumu ("Personal Data Protection Authority"). The Authority’s decision-making body is Kiisel Verileri Koruma Kurulu ("Personal Data Protection Board"), whose duties and powers are regulated under the Regulation on the Working Procedures and Principles of Personal Data Protection Board.

Kiisel Verileri Koruma Kurumu

Nasuh Akar Mah. Ziyabey Cad. 1407. Sok. No: 4
06520 Balgat-Çankaya/Ankara
T +90 312 216 5050
http://www.kvkk.gov.tr

Last modified 24 January 2018

http://www.dlapiperdataprotection.com
REGISTRATION

Pursuant to the LPPD and Regulation on the Registry of Data Controllers, data controllers are required to enrol 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 30 December 2017 and entered into force on 1 January 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 enrolment in the registry.

Under the Regulation, all data controllers are required to enrol in the Data Controllers Registry before proceeding with data processing. However, the Data Protection Board may bring an exception to the obligation of enrolment by taking into account the nature and number of personal data, purpose of processing personal data and some other objective criteria. Also, for the following personal data processing activities, data controllers have no obligation to enrol in the registry and to report these activities:

a. if processing of personal data is required for criminal investigation or for prevention of a criminal offence;
b. if the personal data being processed is already publicized by the data subject;
c. 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

d. 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.

Data controllers who are non-resident in Turkey shall enrol 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 above-mentioned representatives of non-resident data controllers shall, as part of the enrolment procedure, appoint an individual to act as “contact person” for both the Data Protection Authority and for data subjects.

Operations related to the Registry shall be carried out through VERBIS (Data Controllers Registry Information System) by data controllers. Administrative fines of between TRY 20,000 (approx. €4,500) and TRY 1,000,000 (approx. €220,000) may be imposed on data controllers breaching obligations regarding the Registry.

DATA PROTECTION OFFICERS

There is not yet a requirement in Turkey to appoint a data protection officer.

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 personal data must be:

- processed fairly and lawfully;
- accurate and up to date;
- processed for specific, explicit and legitimate purposes;
- relevant, adequate and not excessive; and
- 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; or
• processing is necessary for the legitimate interests of data processor and this does not damage the rights of the data subject.

As part of the collection of data from the data subject the controller is obliged to provide the data subject with the following information:

• the identity of the controller and of his representative, if any;
• the purposes of the processing for which the data is intended;
• the recipients of the data and the reasons for transfer;
• the process of collecting data and the legal grounds, and
• the 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.

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.

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, management and financing of health-care services.

The Regulation on Processing and Protecting the Privacy of Personal Health Data ("Regulation on Health Data") was published in the Official Gazette dated 20 October 2016 and came into force on the same date.

The Regulation on Health Data, as amended, determines rules and procedures for collecting, processing, transferring the personal health data and provides for an access system to be established. It also regulates procedures and principles to be followed in notifying the Ministry of Health of employee movements in relation to the provision of health services. Those who process data shall not copy, save or store the personal health data on any system except the access system established by the Ministry of Health, the central health data system and other data recording environment approved by relevant authorities. The data subject may withdraw the consent for the processing and transfer of the data at any time, if there is no legal regulation or judicial decision otherwise.

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 28 October 2017 and entered into force on 1 January 2018. 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 obliged to determine precautions to be taken for the processing of personal data, 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 at all, the personal data must be deleted, destroyed or anonymized by 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, in the event that conditions for processing personal data contained in the law are no longer met, data controllers 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 DP Law 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 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. Either:

- The country to which personal data will be sent shall have sufficient level of protection; or
- The data controllers in Turkey and in the target country shall undertake protection in writing and obtain the Data Protection Board’s permission.

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 organisational 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.

BREACH NOTIFICATION

There is no general breach notification obligation under the LPPD. However, in the event that personal data is unlawfully obtained by others, the data controller must notify the Personal Data Protection Board and the data subject as soon as possible. If necessary, the Board may declare such situation on its website or in any other way it deems appropriate.

Additionally, under the Regulation on the Protection of Personal Data in the Electronic Communications Sector and the Preservation of Privacy; companies providing electronic communication service and/or providing an electronic communication network and operating the sub-structure ("Operators"), are obliged to inform the Personal Data Protection Authority in a timely and effective manner if there is a risk that violates the security of the network and the personal data.

Administrative fines of up to three percent (3%) of the net sales of the previous calendar year may be applied to the Operator, if the personal data is destroyed, altered, stored or recorded, processed or disclosed involuntarily, in an unauthorized manner or illegally.

ENFORCEMENT

The LLPD and the Turkish Criminal Code No. 5237 impose custodial sentences for the unlawful processing of data. The Turkish Civil Law No. 4721 grants the right to claim compensation for the unjust use of data and a number of other laws impose administrative fines.

Furthermore, the LLPD introduces administrative fines up to TRY 1.000.000 (approx. €227.000) for those who act contrary to the
requirements or rules in the DP Law.

Administrative fines between TRY 5,000 (approx. €1,900) and TRY 20,000 (approx. €4,500) shall be imposed for providers that do not fulfil the obligation of registration to ETBIS.

As mentioned previously, administrative fines between TRY 20,000 (approx. €4,500) and TRY 1,000,000 (approx. €220,000) shall be imposed on data controllers that do not fulfil the registration obligation within the scope of the Regulation on the Registry of Data Controllers.

**ELECTRONIC MARKETING**

The Law on Regulation of Electronic Trade was published in the Official Gazette on 5 November 2014 ("Electronic Trade Law"). The Electronic Trade Law came into force on 1 May 2015. Secondary legislation ("The Regulation on Electronic Trade") was published in the Official Gazette on 26 August 2015 and came into force on the same date.

Pursuant to the Electronic Trade Law, commercial electronic communication (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 form, must contain the recipient's signature. Commercial electronic communications can be sent to craftsmen 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 e-mail, 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.

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 3 business days of the receipt of refusal. Non-compliance with the above obligations is subject to administrative fines between TRY 1,000 to TRY 15,000 TRY (approx. 220 - 3,300 EUR).

The Communiqué on Electronic Trade Information System and Obligations of Notification ("Communiqué") was published in the Official Gazette on 11 August 2017 and entered in force on the same date. The Communiqué regulates the procedure and principles related to the registration and notifications through the Electronic Trade Information System ("ETBIS"), in respect of service providers operating in electronic trade (e-trade) and intermediary service providers that provide e-trade environments for the economic and commercial activities of others. Within the scope of the Communiqué, service providers and intermediary service providers are obliged to enrol in ETBIS before starting e-commerce activities. Service providers and intermediary service providers shall provide information about the service, type of goods and services offered, payment methods and the like.

Similar regulations are enacted under electronic trade law. Accordingly, the obligation of registration and notification to ETBIS is imposed on service providers and intermediaries possessing certain qualifications. With regards to the Communiqué, service providers and intermediary service providers were obliged to fulfil this obligation between 1 December 2017 and 31 December 2017.

Administrative fines between TRY 5,000 (approx. 1,900 EUR) and TRY 20,000 (approx. 4,500 EUR) shall be imposed on providers that do not fulfil the obligation of registration to ETBIS.

The Ministry of Customs and Trade is also empowered to establish an electronic system that allows the receipt of commercial electronic communications approvals and the use of the right to refuse. The approvals received under Electronic Trade Law shall be transferred to the system within the time limit set by the Ministry. The right of rejection by buyers is used through this system. Other procedures and principles regarding the establishment of the system, the transfer of the approvals to the system, the use of the right to refuse, and the operation of the system will be determined by secondary legislation.

**ONLINE PRIVACY**

There is no legislation in Turkey which 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.
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 (3%) of the net sales of the Operator in the previous calendar year shall be imposed if it fails to fulfil its obligation to process traffic data and location data.

---

**KEY CONTACTS**

**Görkem Gökçe**  
Managing Partner  
Gokce Attorney Partnership  
T +90 212 352 88 33  
gorkem.gokce@gokce.av.tr

---

**DATA PRIVACY TOOL**

You may also be interested in our Data Privacy Scorebox to assess your organisation’s level of data protection maturity.
UAE - DUBAI (DIFC)

LAW

Note: Please also see UAE – General.

The DIFC implemented DIFC Law No. 1 of 2007 Data Protection Law in 2007 which was subsequently amended by DIFC Law No. 5 of 2012 Data Protection Law Amendment Law ('DPL').

In addition, under the powers granted to the Commissioner of Data Protection ('CDP') under Article 27 of the DPL, the CDP has issued the Data Protection Regulations ('DPR').

DEFINITIONS

Definition of Personal Data

Any data referring to an Identifiable Natural Person

Definition of Identifiable Natural Person

Is a natural living person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his biological, physical, biometric, physiological, mental, economic, cultural or social identity.

Definition of Sensitive 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.

Definition of Process, Processed, Processes and Processing

Any operation or set of operations which is performed upon Personal Data, 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 or combination, blocking, erasure or destruction.

NATIONAL DATA PROTECTION AUTHORITY

The Commissioner of Data Protection ('CDP') is essentially the regulating body in the DIFC.

The Data Protection Commissioner
Dubai International Financial Centre Authority
REGISTRATION

Unless certain exceptions apply, Data Controllers must obtain a permit from the CDP prior to commencing a Processing Operation involving either Sensitive Personal Data or transferring Personal Data outside of the DIFC.

Data Controllers must also notify the CDP of any Processing operations involving either Sensitive Personal Data or the transfer of Personal Data outside of the DIFC.

DATA PROTECTION OFFICERS

There is no requirement under the DPL or the DPR, for organisations to appoint a data protection officer, though note the general obligation of a Data Controller to implement appropriate technical and organisational measures to protect Personal Data, as further detailed below (see separate Security section).

COLLECTION & PROCESSING

Data Controllers may collect and process Personal Data when any of the following conditions are met:

- the Data Subject has given his/her written consent to the Processing of that Personal Data (DPL, Article 9(a))
- 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 (DPL, Article 9(b))
- processing is necessary for compliance with any legal obligation to which the Data Controller is subject (DPL, Article 9(c))
- processing is necessary for the performance of a task carried out in the interests of the DIFC, or in the exercise of the DIFC Authority, the Dubai Financial Services Authority, the Court and the Registrar’s functions or powers vested in the Data Controller or in a third party to whom the Personal Data are disclosed (DPL, Article 9(d)), or
- processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by the third party or parties to whom the Personal Data is disclosed, except where such interests are overridden by compelling legitimate interests of the Data Subject relating to the Data Subject’s particular situation (DPL, Article 9(1)(e)).

Data Controllers may collect and process Sensitive Personal Data when any of the following conditions are met:

- the Data Subject has given his/her written consent to the Processing of that Sensitive Personal Data (DPL, Article 10(1)(a))
- processing is necessary for the purposes of carrying out the obligations and specific rights of the Data Controller (DPL, Article 10(1)(b))
- 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 consent (DPL, Article 10(1)(c))
- processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association
or any other non-profit-seeking body on condition that the Processing relates solely to the 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 to a Third Party without the consent of the Data Subjects (DPL, Article 10(1)(d))

- the Processing relates to Personal Data which are manifestly made public by the Data Subject or is necessary for the establishment, exercise or defence of legal claims (DPL, Article 10(1)(e))

- processing is necessary for compliance with any regulatory or legal obligation to which the Data Controller is subject (DPL, Article 10(1)(f))

- processing is necessary to uphold the legitimate interests of the Data Controller recognised in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by compelling legitimate interests of the Data Subject relating to the Data Subject’s particular situation (DPL, Article 10(1)(g))

- processing is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter terrorist financing obligations or the prevention or detection of any crime that apply to a Data Controller (DPL, Article 10(1)(h))

- processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those 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 (DPL, Article 10(1)(i))

- processing is required for protecting members of the public against dishonesty, malpractice or other seriously improper, or any resultant financial loss (DPL, Article 10(1)(j)), or

- authorised in writing by the CDP (DPL, Article 10(1)(k)).

**TRANSFER**

Data Controllers may transfer Personal Data out of the DIFC if the Personal Data is being transferred to a Recipient in a jurisdiction that has laws that ensure an adequate level of protection for that Personal Data (DPL, Article 11(1)(a)). An adequate level of protection is when the level of protection in that jurisdiction is acceptable pursuant to the DPR or any other jurisdiction approved by the CDP (DPL, Article 11(2)).

In the absence of an adequate level of protection, Data Controllers may transfer Personal Data out of the DIFC if the:

- CDP has granted a permit or written authorisation for the transfer or the set of transfers and the Data Controller applies adequate safeguards with respect to the protection of this Personal Data (DPL Article 12(1)(a)). Article 5.1 of the DPR then sets out the requirements for applying for such a permit (including a description of the proposed transfer of Personal Data for which the permit is being sought and including a description of the nature of the Personal Data involved)

- data Subject has given his/her written consent to the proposed transfer (DPL Article 12(1)(b))

- 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 (DPL, Article 12(1)(c))

- 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 (DPL, Article 12.1(d))

- transfer is necessary or legally required on grounds important in the interests of the DIFC, or for the establishment, exercise or defence of legal claims (DPL, Article 12.1(e))
• transfer is necessary in order to protect the vital interests of the Data Subject (DPL, Article 12.1(f))

• transfer 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, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case (DPL, Article 12(1)(g))

• transfer is necessary for compliance with any legal obligation to which the Data Controller is subject or the transfer is made at the request of a regulator, police or other government agency (DPL, Article 12(1)(h))

• transfer is necessary to uphold the legitimate interests of the Data Controller recognised in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by legitimate interests of the Data Subject relating to the Data Subject’s particular situation (DPL, Article 12(1)(i)), or

• transfer is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter terrorist financing obligations or the prevention or detection of any crime that applies to a Data Controller (DPL, Article 12(1)(j)).

Authorities who may receive Personal Data in the context of a particular inquiry are not regarded as Recipients under the DPL or the DPRs (as per the definition of Recipient in the DPL).

Safe Harbor Ruling - October 2015

On 26 October 2015 the CDP issued a guidance to DIFC registered entities regarding the adequacy status of US Safe Harbor recipients.

The guidance was issued as a result of a decision by the European Court of Justice (ECJ) on 6 October 2015 which invalidated the European Commission’s Decision 200/520/EC. That EC Decision had provided “adequate protection status” for personal data transfers from European Member States to US Safe Harbor recipients.

As noted above, DPL, Article 11 allows a transfer of personal data out of the DIFC if:

1. an adequate level of protection for that personal data is ensured by the laws and regulations that are applicable to the recipient; or
2. in accordance with DPL, Article 12.

Like the European Commission, the DIFC Data Commissioner had previously listed the US Safe Harbor scheme as a jurisdiction with an "adequate level of protection" on its website. The US Safe Harbor scheme has however now been removed from that list.

The DIFC Data Commissioner’s guidance observes that, as the DIFC Data Protection Laws are largely modelled on relevant EU Directives, the ECJ decision has caused the DIFC Data Commissioner to reconsider the adequacy status previously provided to US Safe Harbor rules. It has noted however that there are currently ongoing negotiations between EU and US authorities regarding the framework.

In light of the above, the DIFC Data Commissioner warns that DIFC organisations should continue to protect individuals’ personal data when transferred to the US and consider potential risks by implementing appropriate legal and technical solutions in a timely manner. DIFC entities transferring personal data to the US should rely upon the conditions referred to in DPL, Article 12 until further clarity is provided.

It is expected that the CDP will release further guidance on how DIFC entities should navigate the Data Protection Law to enable them to legally transfer personal data to the US in the near future.

SECURITY
Data Controllers must implement appropriate technical and organisational measures to protect Personal Data against wilful, negligent, accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of Processing, in particular where Sensitive Personal Data is being Processed or where the Personal Data is being transferred out of the DIFC (DPL, Article 16(1)). When applying for a permit to Process Sensitive Personal Data, or Transfer Personal Data out of the DIFC, Data Controllers must include detail regarding the safeguards employed to ensure the security of such Sensitive Personal Data/Personal Data (respectively, Articles 2.1.1(i) and 5.1.1(i) of the DPR).

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 (DPL, Article 16(2)).

**BREACH NOTIFICATION**

In the event of a breach (being an unauthorised intrusion, either physical, electronic or otherwise, to any Personal Data database, as defined by the DPL) Data Controllers (or Data Processors carrying out a Data Controller’s function at the time of the breach), must inform the CDP of the incident as soon as reasonably practicable (DPL, Article 16(4)).

**ENFORCEMENT**

In the DIFC, the CDP oversees the enforcement of the DPL (DPL, Article 26).

The CDP needs to conduct all reasonable and necessary inspections and investigations before notifying a Data Controller that it has breached or is breaching the DPL or any regulations (DPL, Article 33). If the CDP is satisfied with the evidence of the breach, the CDP may issue a direction to the Data Controller requiring it to do either or both of the following:

- do or refrain from doing any act or thing within such time as may be specified in the direction (DPL, Article 33(1)(a)), or
- 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 (DPL, Article 33(1)(b)).

A Data Controller may ask the CDP to review the direction within fourteen days of receiving a direction and the CDP may receive further submissions and amend or discontinue the direction (DPL, Article 33(6)).

A Data Controller that fails to comply with a direction of the CDP may be subject to fines and liable for payment of compensation (DPL, Article 33(4)).

In addition, if the CDP considers that a Data Controller or any officer of it has failed to comply with a direction, he may apply to the Court for one or more of the following orders:

- an order directing the Data Controller or officer to comply with the direction or any provision of the Law or the Regulations or of any legislation administered by the CDP relevant to the issue of the direction (DPL, Article 33(5)(a))
- an order directing the Data Controller or officer to pay any costs incurred by the CDP or other person relating to the issue of the direction by the CDP or the contravention of such Law, Regulations or legislation relevant to the issue of the direction (DPL, Article 33(5)(b)), or
- any other order that the Court considers appropriate (DPL, Article 33(5)(c)).

Any Data Controller who is found to contravene the DPL or a direction of the CDP may appeal to the DIFC Court within 30 days (DPL, Article 37(1)). The DIFC Court may make any orders that it thinks just and appropriate in the circumstances, including remedies for damages, penalties or compensation (DPL, Article 37(2)).

**ELECTRONIC MARKETING**

As soon as possible upon beginning to collect Personal Data, the DPL requires Data Controllers to provide Data Subjects who they have collected Personal Data from, with, amongst other things, any further information to the extent necessary (having
regard to the specific circumstances in which the Personal Data is collected). This includes information on whether the Personal Data will be used for direct marketing purposes (DPL, Article 13).

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 Processing – 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 Processed or disclosed – provide the Data Subject with, amongst other things, information regarding whether the Personal Data will be used for direct marketing purposes (DPL, Article 14).

Before Personal Data is disclosed for the first time to third parties or used on a Data Subject’s behalf for the purposes of direct marketing, Data Subjects also have the right to be informed and to be expressly offered the right to object to such disclosures or uses (DPL, Article 18).

Additionally, the DPL requires a Data Controller to record various types of information regarding its Personal Data Processing operations (Article 19(4)). This must include an explanation of the purpose for the Personal Data Processing (DPL, Article 6.1.1(b)). The DPR suggests that one of these purposes may be for advertising, marketing and public relations for the Data Controller itself or for others (Article 6.2.1).

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 UAE criminal law applies in the DIFC, the privacy principles laid out therein may apply (see UAE - General section).

KEY CONTACTS

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paul Allen</td>
<td>Head of Intellectual Property &amp; Technology – Middle East</td>
<td></td>
</tr>
<tr>
<td>Eamon Holley</td>
<td>Legal Director</td>
<td>T +971 4 438 6293</td>
</tr>
<tr>
<td>Jamie Ryder</td>
<td>Senior Legal Consultant</td>
<td>T +971 4 438 6297</td>
</tr>
<tr>
<td>Robert Flaws</td>
<td>Senior Legal Consultant</td>
<td>T +971 4 438 6287</td>
</tr>
</tbody>
</table>

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation’s level of data protection maturity.
On 1 January 2017 the UAE’s Central Bank published the Regulatory Framework for Stored Values and Electronic Payment Systems ("Digital Payment Regulation"). This regulation governs digital payment service providers ("PSPs") in the UAE, providing services such as cash-in services, cash out services, retail credit and debit digital payment transactions, government credit and debit digital payment transactions, peer-to-peer digital payment transactions and money remittances. PSPs are required to store all User identification data and transaction records. This data can only be made available to the corresponding User, the Central Bank, to other regulatory authorities following prior approval of the Central Bank, or by UAE court order. PSPs must not process or share the personal data provided by Users, unless necessary as per anti-money laundering ("AML") and combating of financing terrorism ("CFT") laws. PSPs must store and retain all User and transaction data exclusively within the borders of the UAE, excluding UAE financial Free Zones (the DIFC and ADGM), for a period of five (5) years from the date the original transaction. No User or transaction data can be stored outside of the UAE. Details of Users’ personal information must be stored for a minimum of five (5) years from the date the User relationship is terminated.

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.

In addition, there are several UAE Federal Laws that contain various provisions in relation to privacy and the protection of personal data:

- Constitution of the UAE (Federal Law 1 of 1971)
- Penal Code (Federal Law 3 of 1987 as amended)
- Cyber Crime Law (Federal Law 5 of 2012 regarding Information Technology Crime Control), and
- Regulating Telecommunications (Federal Law by Decree 3 of 2003 as amended), which includes several implementing regulations/policies enacted by the Telecoms Regulatory Authority (‘TRA’) in respect of data protection of telecoms consumers in the UAE.
DEFINITIONS

The concept of ‘Personal Data’, as understood in the EU, is not reflected under UAE Federal Law. The corresponding concept within UAE Law encompasses notions such as ‘secrets’, ‘photographs’, ‘the privacy of the individual or family life’ and ‘private life or family life secrets of individuals’. As such, while no UAE Federal Law explicitly states that the collection of personal data requires express consent, if any such data pertains to private or family life then, in certain circumstances, the consent of the individual(s) concerned may be required.

The term ‘Personal Data’ as used below refers to the UAE understanding of the concept as described above.

The Digital Payment Regulation does not define User identification data, however other Central Bank regulations, such as AML and CFT rules, require, for example, that when banks open an account they obtain documentation to include the full name of the account holder, the current address and place of work as well as copies of the account holder’s passport.

NATIONAL DATA PROTECTION AUTHORITY

There is no National Data Protection Authority in the UAE. In respect of telecommunications services, the TRA is responsible for overseeing the relevant telecoms laws and policies.

The UAE Central Bank is responsible for the Digital Payment Regulation.

REGISTRATION

There are no data protection registration requirements in the UAE.

DATA PROTECTION OFFICERS

There is no requirement in the UAE for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

If the collection and processing of any personal data pertains to an individual’s private or family life then the consent of the individual may be required in certain circumstances. A failure to obtain such consent would constitute a breach of the Penal Code (Article 378) and could also be a breach of the:

- Cyber Crime Law if the personal data is obtained or processed through the internet or electronic devices in general (Articles 21 and 22), and
- Telecoms Law to the extent that data is obtained through any means of telecommunication, including through a telecommunications service provider, or any other electronic means. In addition, the facility should be made available for such consent to be withdrawn at a later stage (TRA Consumer Protection Regulations, Article 12.5).

The Cyber Crime Law criminalises obtaining, possessing, modifying, destroying or disclosing (without authorisation) electronic documents or electronic information relating to medical records (Article 7). Additionally, unlawful access via the internet or electronic devices of financial information (eg Credit Cards and Bank Accounts) without permission is an offence under Articles 12 and 13.

TRANSFER

Pursuant to the Penal Code (Article 379), personal data may be transferred to third parties inside and/or outside of the UAE if the data subjects have consented in writing to such transfer, or otherwise where allowed by law.

In addition, in circumstances where telecommunications service providers provide subscriber information to affiliates or third parties directly involved in the supply of the services requested by a subscriber, the third parties are required to take all reasonable and appropriate measures to protect the confidentiality and security of the 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 (TRA Consumer Protection Regulations, Article 13.8).

However, the requirement to obtain written consent may be waived, pursuant to the Penal Code (Article 377), where the personal data pertains to a crime to which the data subject is answerable and it is disclosed in good faith to the relevant authorities.

SECURITY

There are no specific provisions under UAE Federal Law relating to the type of measures to be taken or level of security to have in place against the unauthorised disclosure of personal data. Instead, the 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).

Article 13.1 of the TRA Consumer Protection Regulations requires telecommunications service providers to ‘take all reasonable and appropriate measures to prevent the unauthorised disclosure or the unauthorised use of subscriber information’. Article 13.3 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 form’, and that ‘reliable security measures’ should be employed.

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

In principle, there is no mandatory requirement under UAE Federal Law to report data security breaches.

Data subjects based in the UAE, however, may be entitled to hold the entities in possession of their data, liable under the principles of the UAE Civil Code for their negligence in taking proper security measures to prevent the breach, if such breach has resulted in actual losses being suffered by the data subjects.

In relation to telecommunication services, the Telecoms Law and most Policies do not include an explicit requirement on service providers to take the initiative in notifying the TRA of a breach or alleged breach, unless a subscriber complains to a service provider about the unauthorised disclosure of his or her personal data. Such a notification would be included in the monthly reporting which is submitted to the TRA (Article 15.10.2 of the TRA Consumer Protection Regulations).

Subscribers are also able to complain directly to the TRA about the unauthorised disclosure of their personal data. However, the TRA will generally only handle subscriber complaints after the complaint has been submitted to the service provider and if the matter has not been satisfactorily resolved by the service provider’s own customer complaints procedure (Article 15.11.1 of the TRA Consumer Protection Regulations and Article 1.1 to 1.3 of the TRA Consumer Dispute Procedure).

ENFORCEMENT

There are four possible methods of enforcement from a UAE law perspective:

1. **Where the unauthorised disclosure of personal data results in a breach of the Penal Code:**

   The Public Prosecutor in either the Emirate:

   - where the party suspected of the breach (‘Offender’) resides
   - where 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 the Penal Code (Article 379), if the Courts find a suspect guilty of disclosing secrets that were entrusted to him 'by reason of his profession, craft, situation or art' the penalties to be imposed under the Penal Code may include 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. More generally, pursuant to the Penal Code (Article 378), 'a punishment of confinement and fine shall be inflicted on any person who attacks the sanctity of individuals' private or family life' by committing any of the acts described under Article 378 'other than the legally permitted cases or without the victim'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 1,000,000 (Articles 2, 3, 7, 21 and 22 of the Cyber Crime Law). 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 40).

3. Where the unauthorised disclosure of personal data results in a breach of the Telecoms Law and Policies:

The TRA is responsible for overseeing the enforcement of the Telecoms 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 TRA may be accepted by them at their discretion (Article 14.11.1 of the TRA Consumer Protection Regulations).

The subscriber’s complaint needs to be submitted to the TRA 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 TRA (Article 14.11.1 of the TRA Consumer Protection Regulations).

After examining the complaint the TRA may direct the service provider ‘to undertake any remedy deemed reasonable and appropriate’ (Article 14.11.5 of the TRA Consumer Protection Regulations).

4. Where the unauthorised disclosure or transfer of personal data results in a breach of the Digital Payment Regulation:

The Central Bank will issue administrative penalties against PSPs. Currently the Digital Payment Regulation does not specify the administrative penalties.

ELECTRONIC MARKETING

There are no general laws in the UAE law covering electronic marketing, however the TRA has issued a regulation governing telecommunications licensees’ electronic communications with subscribers, as well as how they should monitor spam passing through their networks. Articles 21 and 22 of the Cyber Crime Law and Article 13.5 of the TRA’s Consumer Protection Regulation, as described in the ‘Collection and Processing’ section above, are also worded widely enough to potentially apply to electronic marketing. Article 22 of the Cyber Crime Law, for example, prohibits the use of various electronic devices in order to disclose, without permission, confidential information that has been obtained through the course of a person’s duties.

The TRA’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.

ONLINE PRIVACY

Although the UAE Penal Code 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 378 as described above).

Additionally, as described in the ‘Collection and Processing’ section above, under certain circumstances, online privacy is protected through Articles 21 and 22 of the Cyber Crime Law and the TRA’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 also an offence under the Cyber Crime Law (Articles 12 and 13).
KEY CONTACTS

Paul Allen
Head of Intellectual Property & Technology – Middle East
T +971 4 438 6295
paul.allen@dlapiper.com

Eamon Holley
Legal Director
T +971 4 438 6293
eamon.holley@dlapiper.com

Jamie Ryder
Senior Legal Consultant
T +971 4 438 6297
jamie.ryder@dlapiper.com

Robert Flaws
Senior Legal Consultant
T +971 4 438 6287
robert.flaws@dlapiper.com

DATA PRIVACY TOOL

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

Last modified 24 January 2018

LAW

The Law of Ukraine No. 2297 VI 'On Personal Data Protection' as of 1 June 2010 (Data Protection Law) is the main legislative act regulating relations in the sphere of personal data protection in Ukraine. At 20 December 2012 Data Protection Law has been substantially amended by the Law of Ukraine 'On introducing amendments to the Law of Ukraine "On personal data protection" dated 20 November 2012 No. 5491-VI. Additional significant changes to Data Protection Law were envisaged by the Law of Ukraine 'On Amendments to Certain Laws of Ukraine regarding Improvement of Personal Data Protection System' dated 3 July 2013 No. 383-VII which came into force on 1 January 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 at 28 January 1981 and the Additional Protocol to the Convention regarding supervisory authorities and trans border data flows, executed in Strasbourg at 8 November 2001 have also been ratified by Ukrainian Parliament at of 6 July 2010 (Convention on Automatic Processing of Personal Data) and thus fully effective in Ukraine.

Besides, the general data protection issues are regulated by:

- the Constitution of Ukraine dated 28 June 1996
- the Civil Code of Ukraine dated 16 January 2003 No 435 IV
- the Law of Ukraine 'On Information' dated 2 October 1992 No 2657 XII
- the Law of Ukraine "On Electronic Commerce" dated 3 September 2015 No 675-VIII; and
- some other legislative acts.
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’ as such envisaged by Ukrainian legislation.

At the same time, 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 offences or conviction to criminal punishment as well as data relating to health or sex life of an individual.

Processing of the listed data is allowed if an 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 1 January 2014 Ukrainian Parliament’s Commissioner for Human Rights (Ombudsman) is the state authority in charge of controlling the compliance with the data protection legislation.

REGISTRATION

Starting from 1 January 2014 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 thirty working days from commencement of such processing. Pursuant to the Notification Procedure, the following types of personal data processing requires obligatory notification of the Ombudsman processing of personal data on:

- racial, ethnic, national origin
- political, religious ideological beliefs
- participation in political parties and/or organisations, trade unions, religious organisations or civic organisation of ideological direction
- state of health
- sexual life
- biometric data
- genetic data, and
- bringing to 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; and
- 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, and
- general description of technical and organisational measures taken by personal data owners in order to maintain the security of personal data.

Where any of the information listed above is submitted to the Ombudsman and has been 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 on termination of personal data processing which is of particular risk to the rights and freedoms of personal data subjects within 10 days from the moment of such termination.

Furthermore, the Notification Procedure obliges the owners and processors of personal data processing the 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 organisation of work related to the protection of personal data during the processing thereof. Such notification shall be made within 30 days from the moment 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**

Legal entities shall establish a special department or appoint a responsible person (data protection officer) to organise the work related to the protection of personal data during the processing thereof.

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 position. There are no particular penalties for incorrect appointment of Data Protection Officer.

**COLLECTION & PROCESSING**

The Data Protection Law provides for a requirement of obtaining the consent of personal data subjects on processing their personal data. According to the Data Protection Law the consent of personal data subject shall mean voluntary expression of will of the individual (subject to his/her awareness) to permit the processing of personal data for the determined purposes, expressed in writing or in some other form which allows the owner or processor of the personal data to make a conclusion that a consent has been granted. In the area of e-commerce, consent regarding processing of personal data may be granted in the process of registration of data subjects by “ticking” the respective box for giving consent on processing of their personal data for the determined processing purposes, provided that such a system does not allow processing of personal data before the consent from the data subject. In some instances provided by Data Protection Law (eg legislative permission for processing of personal data, conclusion and execution of a transaction in favour of the personal data subject, protection of interests of the subject or owner of personal data) personal data of individuals may be processed without the consent.

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
- composition and content of their personal data being collected
- their rights
- 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 10 working days from the moment of their personal data’s collection:

- legislative permission of the owner of personal data on processing of personal data exclusively for the purposes of fulfilling its authorities
• conclusion and execution of a transaction, in which the subject of personal data is a party or which has been concluded in
favour of the subject of personal data or for taking actions, which preceded conclusion of a transaction at the request of
the subject of personal data

• protection of vital interests of the subject of personal data, or

• need to protect legitimate interests of the owner of personal data, third parties, except where a subject of personal data
demands to stop the processing of his/her personal data and the need in protection of personal data prevails over such
interest.

In addition, the Data Protection Law provides the subject of personal data 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 as regards the conditions of providing access to personal data, 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 receipt of his/her request, informing the individual whether
his/her personal data are being processed and to receive the contents of such personal data

• to provide the owner of personal data with the reasonable request to terminate 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 unauthorised processing and accidental loss, elimination or damage with respect
to intended encapsulation, not providing or the untimely providing of personal data, and also to protection 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 processing of personal data, and

• to be protected from the automated decision that has legal effect on it.

The owner of the personal data can entrust the processing of personal data to the processor of personal data under the written
agreement between them. In this case the processor of personal data may process the personal data only for the purposes and in
the volume provided by such agreement. The transfer of personal data to the processor of personal data can be allowed only by
respective consent of the personal data subject.

TRANSFER

In accordance with Data Protection Law the personal data may be transferred to foreign counterparties only on condition of
ensuring an appropriate level of protection of personal data by 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 favour of the personal data subject
- necessity to protect the vital interests of the personal data subjects
- necessity to protect public interest, establishing, fulfilling and enforcing of a legal requirement, or
- appropriate guarantees of the personal data owner as regards non-interference in personal and family life of the personal data subject.

SECURITY

The subjects of personal data relations are obliged to take appropriate technical and organisational measures to ensure the protection of personal data against unlawful processing, including against loss, unlawful or accidental elimination, and also against unauthorised access. In this regard, any owner of personal data shall determine a special department or a responsible person to organise the work related to the protection of personal data during the processing thereof.

The Model Procedure stipulates that the owners and processors of personal data shall take measures to maintain security of personal data on all stages of their processing including organisational and technical measures for the protection of personal data. Organisational measures shall include:

- determination of a procedure of access to personal data by employees of the owner/processor of personal data
- determine the order of recording of operations related to the processing of personal data of the subject and access to them
- elaboration of an action plan in case of unauthorised access to personal data, damage of technical equipment or occurrence of emergency situations, and
- regular trainings of employees which are working with personal data.

Personal data irrespective of the manner of its storage shall be processed in the way which makes unauthorised 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 unauthorised access to personal data being processed and ensure 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 the state authorities responsible for controlling the compliance with personal data protection legislation. Failure to comply with the provisions of Data Protection Law can lead to responsibility prescribed by 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 can be obliged 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 on the processing of personal data or on a change of information submitted which is subject to notification under Ukrainian legislation, or submission of incomplete or false information may lead to a fine of up to EUR 197
- non-fulfilment of legitimate requests (orders) of the Ombudsman or determined state officials of the Ombudsman's secretariat as regards the elimination or prevention of violations of personal data protection legislation may lead to a fine of up to EUR 491
- non-fulfilment of legitimate requests of Ombudsman or its representatives may lead to a fine of up to EUR 94
- non-observance of the established procedure for the protection of personal data which leads to unauthorised access to the personal data or violation of rights of the personal data subject may lead to a fine of up to EUR 491.

The criminal liability, prescribed by the Criminal Code of Ukraine envisages fines of up to EUR 491 or correctional works for a term of up to two years, or 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 3 September 2015 provides for certain legal requirements for distribution of commercial electronic messages in the area of electronic commerce. 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 refuse from receiving of 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: (i) full name of legal entity/individual; place of registration/residence; (ii) email/web-site of online shop; (iii) registration number or tax ID number/passport details (for individuals); (iv) licence data (in case if it is mandatory under the law); (v) inclusion of taxes in calculation of the price of goods/services; and (vi) price of delivery of goods (in case if delivery is performed)); and
- commercial electronic messages regarding sales, promotional gifts, premiums etc. shall be unequivocally identified as such and conditions of receiving of such promotions shall be clearly stated to avoid their ambiguous understanding as well as shall comply with advertising legislation.

When electronic marketing involves the processing of an individual's personal data, it should take place in compliance with the requirements of Ukrainian data protection legislation.

Considering the requirements of the Data Protection Law outlined above, in order for the use of an individual’s personal data for electronic marketing purposes, there is a requirement to obtain appropriate consent from the individual which would allow for the processing of his / her personal data for such purposes.

**ONLINE PRIVACY**

There is no specific legislation regulating the sphere of online privacy in Ukraine. However, the Data Protection Law applies to the
extent online activities involve the processing of personal data.

**KEY CONTACTS**

**Natalia Pakhomovska**  
Partner  
T +380 44 495 1789  
natalia.pakhomovska@dlapiper.com

**Natalia Kirichenko**  
Senior Associate  
T +380 44 490 9575  
natalia.kirichenko@dlapiper.com

**DATA PRIVACY TOOL**

You may also be interested in our Data Privacy Scorebox to assess your organisation’s level of data protection maturity.
DATA PROTECTION LAWS OF THE WORLD

UNITED KINGDOM

Last modified 24 May 2018

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 GDPR will come into force in the United Kingdom on 25 May 2018, on which date the UK will continue to be a Member State of the European Union.

Alongside the GDPR, the United Kingdom has prepared a new national data protection law, the Data Protection Act 2018 ("DPA"), which also comes into force on 25 May 2018. As well as containing derogations and exemptions from the position under the GDPR in certain permitted areas, the DPA also does the following:

• allows for the continued application of the GDPR in UK national law once the UK leaves the European Union (expected to be 29 March 2019);
• 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.
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 expressions used in the GDPR. For the purposes of the UK, 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

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 Information Commissioner (whose functions are discharged through the Information Commissioner’s Office ("ICO")) is the supervisory authority for the UK for the purposes of art. 51 of the GDPR.
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

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 accordance with the position advocated by recital 89 of the GDPR, the UK’s system of general registration for controllers will be abolished from 25 May 2018.

However, the UK has opted to replace the system of general registration with a fee-paying scheme for controllers, known as the Data Protection Fee. Controllers will have to pay an annual data protection fee to the ICO, unless they are exempt from doing so.

Those controllers who have an unexpired registration under the old system will not be required to pay the new fee until their existing registration expires, at which point the ICO will contact them with details of the new fee.

Parliament has set the fees 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 £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 £4,350 (150% of the top tier fee).

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 UK has not opted to extend the requirement to appoint a Data Protection Officer.

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 .xml).

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. 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.

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. Parts 1 and 2 of Schedule 1 to the DPA provide a number of such bases, in the form of ‘conditions’, which in effect provide UK specific gateways to legalise the processing of certain types of special category data. Many of these conditions are familiar from the previous UK law, whilst other are new. Important examples include:

- processing required for employment law;
- health 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 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 GDPR in relation to this more sensitive processing data activity.

Child'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 the UK.

Automated Decision Making (Article 22)

Article 22(2)(b) of the GDPR allows member states to authorise automated decision making in local law, subject to additional safeguards, for purposes beyond the two permitted gateways already set out in Article 22(2) of the GDPR (ie, explicit consent, or necessity for entering into or performance of a contract with the data controller).

The DPA takes advantage of this provision to enable automated decision making where the automated decision is accompanied by the sending of a specific notice to the data subject which provides them with a one month period to request the controller to (i) reconsider the decision, or (ii) take a new decision that is not based solely on automated processing.

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.

Once the UK leaves the EU (expected to be the 29 March 2019) it will become a third country for the purposes of Chapter V of the GDPR. It is possible that the UK will achieve an adequacy decision to coincide with its date of exit (such a decision would not be surprising, given the UK’s desire to continue applying the GDPR). However, in the absence of an adequacy decision, alternative safeguards would technically be required to transfer personal data from the EU to the UK. This area remains uncertain, and it is recommended that organisations closely monitor the unfolding picture in respect of the UK / EU negotiations.

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.

---

Personal data breaches should be notified to the ICO, as the UK’s supervisory authority. Breaches 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 is preferred) a pro forma may be downloaded and emailed to the ICO.

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 DPA sets out the specific enforcement powers provided to the ICO pursuant to Article 58 of the 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
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 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, a change which is currently forecast for Spring 2019. 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 (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 provides individuals with the right to prevent the processing of their personal data (e.g. a 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 ICO using his powers under the Act.

The PEC Regulations prohibit the use of automated calling systems without the consent of the recipient. The PEC Regulations also prohibit unsolicited electronic communications (i.e. 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.

**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 has confirmed that consent can be implied where a user proceeds to use a site after being provided with clear notice (e.g. by way of a pop-up or banner) that use of site will involve installation of a cookie.

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 and sanctions for breach are the same as set out in the enforcement section above.

**KEY CONTACTS**

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

Ross McKean  
Partner  
T +44 (0) 20 7796 6077  
ross.mckean@dlapiper.com
DATA PRIVACY TOOL

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

LAW

The United States has about 20 sector specific or medium-specific national privacy or data security laws, and hundreds of such laws among its 50 states and its territories. (California alone has more than 25 state privacy and data security laws). These laws, which address particular issues or industries, are too diverse to summarize fully in this volume.

In addition, the large range of companies regulated by the Federal Trade Commission ("FTC") are subject to enforcement if they engage in materially unfair or deceptive trade practices. The FTC has used this authority to pursue companies that fail to implement reasonable minimal data security measures, fail to live up to promises in privacy policies, or frustrate consumer choices about processing or disclosure of personal data.

DEFINITIONS

Definition of personal data

Varies widely by regulation. The FTC now considers information that can reasonably be used to contact or distinguish a person, including IP addresses and device identifiers, as personal data. However, very few U.S. federal or state privacy laws define "personal information" as including information that on its own does not actually identify a person.

Definition of sensitive personal data

Varies widely by sector and by type of statute. Generally personal health data, financial data, credit worthiness data, student 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. For example, US state data security breach notice and state data security laws typically cover name plus government identification number, financial account or payment card number, and in some states health insurance medical and/or biometric data, and user name and password for an online account.

NATIONAL DATA PROTECTION AUTHORITY

No official national authority. However, the FTC has jurisdiction over most commercial entities and has authority to issue and enforce privacy regulations in specific areas (eg for telemarketing, commercial email, and children’s privacy). The FTC uses its general authority to prevent unfair and deceptive trade practices to bring enforcement actions against inadequate data security measures, and inadequately disclosed information collection, use and disclosure practices. State attorneys general typically have similar authority and bring some enforcement actions, particularly in the case of high profile data security breaches.

In addition, a wide range of sector regulators, particularly those in the health care, financial services, communications, and insurance sectors, have authority to issue and enforce privacy regulations.

REGISTRATION
There is no requirement to register databases.

**DATA PROTECTION OFFICERS**

With the exception of entities regulated by HIPAA, there is no requirement to appoint a data protection officer, although appointment of a chief privacy officer and an IT security officer is a best practice among larger organisations and increasingly among mid sized ones. In addition, Massachusetts law requires an organization to appoint one or more employees to maintain its information security program. The law applies to organizations that own or license personal data on residents of Massachusetts, and thus reaches outside the state.

**COLLECTION & PROCESSING**

US privacy laws and self regulatory principles vary widely, but generally require pre collection notice and an opt out for use and disclosure of regulated personal information.

Optin rules apply in special cases involving information that is considered sensitive under US law, such as for health information, use of credit reports, student data, personal information collected online from children under 13 (see below for the scope of this requirement), video viewing choices, precise geolocation data, and telecommunication usage information. The FTC interprets as a "deceptive trade practice" failing to obtain opt in consent if a company engages in materially different uses or discloses personal information not disclosed in the privacy policy under which personal information was collected. It has, for example, sued to prevent disclosure of personal data as part of several bankruptcy proceedings.

States impose a wide range of specific requirements, particularly in the employee privacy area. 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.

The US also regulates marketing communications extensively, including telemarketing, text message marketing, fax marketing and email marketing (which is discussed below). The first three types of marketing are frequent targets of class action lawsuits for significant statutory damages.

**TRANSFER**

No geographic transfer restrictions apply in the US, except with regard to storing some government information. The Commerce Clause of the U.S. Constitution likely bars US states from imposing data transfer restrictions and there are no other such restrictions in US national laws.

Please note that following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C362/14) the USEU safe harbor regime is no longer regarded as a valid basis for transferring personal data to the US.

**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, or information that would require security breach notification). A few states have enacted laws imposing more specific security requirements for data elements that trigger security breach notice requirements. For example, Massachusetts has enacted regulations which 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; the regulations also set forth the minimum components of such program, including binding all service providers who touch this sensitive personal information data to protect it in accordance with the regulations. Both Nevada and Massachusetts laws impose 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.

HIPAA regulated entities are subject to much more extensive data security requirements, and some states impose further security requirements (eg for payment card data, for social security numbers, or to employ secure data destruction methods). HIPAA security regulations apply to so-called ‘covered entities’ such as doctors, hospitals, insurers, pharmacies and other health-care
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.

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.

BREACH NOTIFICATION

Security breach notification requirements are a US invention. 47 US states, Washington, D.C. and most US territories (including, Puerto Rico, Guam and the Virgin Islands) require notifying state residents of a security breach involving residents’ name plus a sensitive data element typically, social security number, other government ID number, or credit card or financial account number. In a growing minority of states, sensitive data elements also include medical information, health insurance numbers, biometric data, and login credentials (ie username and password). Also, date of birth, tax ID, shared security “secrets”, and birth and marriage certificates are each considered sensitive data under the breach notice laws of at least one state.

Notice of larger breaches is typically required to be provided to credit bureaus, and in minority of states, to State Attorneys Generals and/or other state officials. Federal laws require notification in the case of breaches of health care information, breaches of information from financial institutions, breaches of telecomm usage information held by telecomm services, and breaches of government agency information.

ENFORCEMENT

Violations are generally enforced by the FTC, State Attorneys General, or the regulator for the industry sector in question. Civil penalties are generally significant. In addition, some privacy laws (for example, credit reporting privacy laws, electronic communications privacy laws, video privacy laws, call recording laws, cable communications privacy laws) are enforced through class action lawsuits for significant statutory damages and attorney’s fees. Defendants can also be sued for actual damages for negligence in securing personal information such as payment card data, and for surprising and inadequately disclosed tracking of consumers.

ELECTRONIC MARKETING

The US regulates marketing communications extensively, including email and text message marketing, as well as telemarketing and fax marketing.

E-mail

The CAN-SPAM Act is a federal law that applies labelling 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. Not only the FTC and State Attorneys General, but also ISPs and corporate email systems can sue violators. Furthermore, 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) needs to be carefully reviewed for strict compliance with legal requirements.

Telemarketing
In general, federal law applies to most telemarketing calls and programs, and a state’s 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. For example, national (‘federal’) and state rules address calling time restrictions, honouring do-not-call registries and opt-out requests, mandatory disclosures to be made during the call, requirements for completing a sale, executing a contract or collecting payment during the call, 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.

Callers generally must scrub their calling lists against both a national and multiple state do-not-call registries, as it is prohibited to place a telemarketing call to a number listed in a do-not call registry unless a specific exemption applies. The national do-not-call rules (and several state rules), for example, exempt calls to existing business customers who have purchased a product or service in the last 18 months from the company on whose behalf the call is placed, as long as the customer has not specifically opted out of receiving telemarketing calls from the company. The use of auto-dialers to send pre-recorded messages generally requires affirmative opt-in consent of the recipient.

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 hasn’t 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.

ONLINE PRIVACY

Online Privacy Policy Requirement

The States of California and Delaware require commercial online websites and mobile applications to post a relatively general online privacy policy. Liability for failing to post the privacy policy may only be imposed if the website or mobile app is notified of its non-compliance and fails to post the policy with 30 days of receiving notice of non-compliance.

Cookies

There is no specific federal law that regulates the use of cookies, web beacons, Flash LSOs and other similar tracking mechanisms. However, the Children’s Online Privacy Protection Act (COPPA) applies to information collected automatically (eg via cookies) from child-directed websites and other websites and third party ad networks or plug-ins that knowingly collect personal information online from children under 13, COPPA also regulates behavioural advertising to children under 13.

In addition, undisclosed online tracking of customer activities poses class action risk. The use of cookies and similar tracking mechanisms should be carefully and fully disclosed in a website privacy policy. Furthermore, it is a best practice for websites that allow behavioural advertising on their websites to participate in the Digital Advertising Alliance code of conduct, which includes displaying an icon from which users can opt out of being tracked for behavioural advertising purposes. 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 honours any ‘Do-Not-Track’ method or provides users a way to opt out of such tracking; however, the law does not mandate that companies provide consumers a ‘Do-Not-Track’ option. 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).

**Minors**

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.

**Location Data**

Privacy requirements of location based apps and services is in flux and is a subject of extensive interest and debate. Federal Communications Commission regulations govern the collection and disclosure of location information by telecommunications carriers, including wireless carriers. Further, any location service that targets children under the age of 13 or has actual knowledge that it is collecting location information from children under age 13 must comply with the requirements of the COPPA Rules including obtaining prior verifiable parental consent in most circumstances. Both the Federal Trade Commission and California Attorney General’s Office have issued best practices recommendations for mobile apps and mobile app platforms, and the California Attorney General has entered into an agreement with major app platforms in which they promise to prompt mobile apps to post privacy policies. Furthermore, a Department of Commerce led multi stakeholder negotiation to develop a code of conduct for mobile app privacy is well underway.

**KEY CONTACTS**

| Jim Halpert |
| Partner & Chair of US Data Protection and Privacy Group |
| T +1 202 799 4441 |
| jim.halpert@dlapiper.com |

| Jennifer Kashatus |
| Partner, Data Protection, Privacy and Security |
| T +1 202 799 4448 |
| jennifer.kashatus@dlapiper.com |

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

**DATA PRIVACY TOOL**

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

LAW

Data Protection Act Law No. 18.331 (11 August 2008); Decree No. 414/009 (31 August 2009) (the ‘Act’).

DEFINITIONS

Definition of personal data

Any kind of information related to an identified or identifiable person or legal entity.

Definition of sensitive personal data

Any kind of personal data evidencing: racial or ethnic origin, political preferences, religious or moral beliefs, trade union membership as well as any kind of information concerning health or sexual life.

NATIONAL DATA PROTECTION AUTHORITY

(‘URCDP’, Unidad Reguladora y de Control de Datos Personales (‘Data Protection Authority’).

REGISTRATION

Every database must be registered with the Data Protection Authority in Uruguay if the information contained in the database is gathered or obtained through means, mechanisms or sources located in Uruguay.

The database must be registered by filing mandatory forms, which must be signed by a representative of the company that owns the data base.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION & PROCESSING

In order to collect personal data contained in a database, the data processor must first 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 address, telephone number, ID number, nationality, tax number, corporation name
personal data obtained based on a contractual or professional relationship, which is necessary to perform the contract or the development of the professional services to be rendered, or

- personal data obtained by individuals or corporations for their personal and exclusive use.

The personal data processed cannot be used for secondary purposes, which are different from those that have justified the initial acquisition of the information. There must be legitimate reasons (i.e., reasons which are not against the law) for the processing of the personal information. The Act further establishes that once the reasons to process the personal information are no longer present, the personal information must be deleted.

**TRANSFER**

Personal data can only be transferred to a third party:

- for purposes directly related to the legitimate interests of the transferring party and the transferee, and

- with the prior consent of the data subject. However, such consent may be revoked. Additionally, the data subject must be informed of the purpose of the transfer, as well as of the identity of the recipient.

However, the prior consent of the data subject is not necessarily required when the personal 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 request for consent 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 severally liable for the compliance of the recipient’s obligations under the Act.

The Act forbids the transfer of personal data to countries or international entities which do not provide adequate levels of protection (according to European standards). However, the 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 provide for 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 recipient branch has adopted a conduct of code duly registered with 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 code of conduct (such as an inter-company agreement) duly filed with URCDP.

**SECURITY**

Data processors must implement appropriate technical and organisational measures to guarantee the security and confidentiality of the personal data. These measures should be aimed at preventing the loss, falsification, and unauthorised treatment or access, as well as at detecting information that may have been lost, leaked, or accessed without authorisation.

It is prohibited to register personal data in databases which do not meet technical safety conditions.

**BREACH NOTIFICATION**
In case the data processor detects a breach of security measures, and if the consequences of the breach could substantially affect the rights of the data subject and/or the rights of any other agent or person involved, the data processor should report the breach to the affected persons.

**ENFORCEMENT**

The URCDP is responsible for enforcement of the Act. In the context of its powers, the URCDP has broad investigatory powers, including audit and inspection rights, and subpoena, search and seizure authority.

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 database for five days, closure of the database.

**ELECTRONIC MARKETING**

The Act will apply to most electronic marketing activities, as these activities typically 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/data subjects (individuals or legal entities) the right to demand the deletion or suppression of their data from the marketing database.

Personal data may be used and processed for marketing purposes when the personal data was either obtained from public documents, provided by the data subject or when prior consent has been gathered.

**ONLINE PRIVACY**

There are no provisions that specifically address online tracking or geolocation data. However, the general principles of the Act apply. The personal data processed cannot be used for purposes other than those that justified the acquisition of the data; and when the reasons to process the personal information have expired, the personal information must be deleted.

**KEY CONTACTS**

**Estudio Bergstein**

www.bergsteinlaw.com/

**Jonas Bergstein**

Partner

T +598 2 901 2448

jbergstein@bergsteinlaw.com

**Guzmán Ramírez**

T +598 2901 2448

gramirez@bergsteinlaw.com

**DATA PRIVACY TOOL**

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

The protection of privacy is a principal enshrined in Zimbabwe's Constitution. Whilst there is no designated national legislation dealing with data protection for private persons in Zimbabwe yet, there are existing laws that have a bearing on the right to privacy and protection of personal information for specified types of data, or in relation to specific activities.

The Access to Information and Protection of Privacy Act (Chapter 10:247) is the law which contains the most provisions on data protection. However, this generally only regulates the use of personal data by public bodies.

Other laws refer to the protection of information as a function of other activities or the protection of specific types of data such as the Courts and Adjudicating Authorities (Publicity Restrictions) Act (Chapter 07:04), the Census and Statistics Act (Chapter 10:29), Banking Act (Chapter 24:20), National Registration Act (Chapter 10:17) and the Interception of Communications Act (Chapter 11:20).

In August 2016 Cabinet, which is the highest government approval body, approved the Revised ICT Policy. According to the approved ICT policy, the establishment of an institutional framework for enacting legislation dealing specifically with digital data protection matters and cyber security is anticipated.

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 health care 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 which defines sensitive personal data.
NATIONAL DATA PROTECTION AUTHORITY

There is no data protection authority. However, the Zimbabwe Media Commission’s mandate does include the following:

- ensuring that the people of Zimbabwe have equitable and wide access to information
- commenting on the implications of proposed legislation or programmes of public bodies on access to information and protection of privacy
- commenting on the implications of automated systems for collection, storage, analysis or transfer of information or for the access to information or protection of privacy
- amongst other functions.

The approved 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 set up.

REGISTRATION

There is no law that requires the registration of databases.

DATA PROTECTION OFFICERS

There is no provision to appoint data protection officers.

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.

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 authorised to collect, compile, analyse and abstract statistical information relating to the:

- commercial
- industrial
- agricultural
- mining
- social
- economic
- and general activities and conditions of the inhabitants of Zimbabwe and to publish such statistical information.

TRANSFER

The transfer of personal data to any other jurisdiction is not specifically restricted.

SECURITY

The approved ICT policy states that there will be development, implementation and promotion of appropriate security and legal systems for e-commerce including issues related to cyber security, 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: (i) data protection and privacy (ii) Intellectual property protection and copyright (iii) consumer protection and (iv) child online protection.
BREACH NOTIFICATION

Breach notification

There is no law which requires data protection officers to report a breach.

Mandatory breach notification

There are no mandatory breach notification provisions.

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 enshrined as a basic human right, which therefore falls within the purview of the HRC. However, the Monitoring of Interception of Communications Centre (MICC), 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 MICC 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.

ELECTRONIC MARKETING

The Government is currently working on a Consumer Protection Act, which seeks to protect consumers from unfair trade practices. The draft Consumer Protection Bill does not make reference to electronic marketing, nor does it provide for consumer privacy rights in respect of personal data.

ONLINE PRIVACY

There is currently no specific online privacy legislation.

KEY CONTACTS

Manokore Attorneys
www.corporatecounsel.co.zw

Bridget Mafusire
Associate
T +263 4 746 787
bmafusire@corporatecounsel.co.zw

Lloyd Manokore
Partner
T +263 4 746 787
lmanokore@corporatecounsel.co.zw

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation’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 © 2017 DLA Piper. All rights reserved.