

DATA PROTECTION LAWS OF THE WORLD

Cyprus



Downloaded: 19 April 2024

CYPRUS



Last modified 21 February 2022

LAW

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

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

Territorial Scope

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

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

The Protection of Physical Persons Against the Processing of Personal Data and Free Movement of such Data Law 125(I)/2018, that implements certain provisions of the GDPR into local law, entered into force on July 31, 2018 (the **Law**).

DEFINITIONS

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

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

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

convictions and offences (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

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

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

The Law uses the definitions provided under the GDPR without any derogation.

NATIONAL DATA PROTECTION AUTHORITY

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

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

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

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

The authority designated under the Law as being the local regulatory body for the purposes of the GDPR is the Commissioner for the Protection of Personal Data in Cyprus (the **Commissioner**).

The Law affords certain powers to and imposes obligations on the Commissioner which are in addition to the GDPR, including, inter alia, the following:

- Examination of complaints and providing information to the person making the complaint within 30 days of submission thereto.
- The obligation to inform the data subject, the data controller and the processor of the deadlines indicated under Articles 60-66 of the GDPR.
- The publication of a list of processing activities requiring the appointment of a data protection officer.
- To consult specialists or the police for exercising its regulatory powers under Article 58 of the GDPR.
- To enter, without giving any prior notice to the data controller or the processor or their representatives, any office, business premises or means of transport with the exception of housing premises, for inspections.
- To inform the Attorney General's Office and / or the police for breaches of the GDPR and the national law giving rise to criminal liability.
- To permit the combination of filing systems and to impose terms and conditions in relation thereto.
- To impose terms and conditions to the exemption from the obligation of the data controller to notify data

subjects for breaches of personal data as provided for in Article 23 of the GDPR.

- To impose explicit restrictions on the transfer of special categories of personal data to third countries or international organizations.

Further, the Certification Body for the purposes of Article 43 of the GDPR is the Cyprus Organisation of the Promotion of Quality which is the national organization for accreditations in Cyprus operating under the Standardisation, Accreditation and Technical Notification Law (LI56(I)/2002).

REGISTRATION

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

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

There is no registration applicable with the exception of what is referred to in the immediately succeeding paragraph for data protection officers.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

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

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

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

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

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

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;

- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

According to the Law, the Commissioner may draw up and make available to the public a list of the processing operations and / or other instances which shall deem necessary the designation of a data protection officer (the DPO) by the data controller and the processor. A list of names of data controllers and processors who have designated a DPO may be published on the Commissioner's website provided the data controller and the processor wish to be included therein.

COLLECTION & PROCESSING

Data Protection Principles

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

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

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

Legal Basis under Article 6

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

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

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

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

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

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

Processing for a Secondary Purpose

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

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

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

Transparency (Privacy Notices)

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

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

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

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

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

Rights of the Data Subject

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

Right of access (Article 15)

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

Right to rectify (Article 16)

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

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

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

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

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the

accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (eg, commonly used file formats recognized by mainstream software applications, such as .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 making, including profiling (Article 22)

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

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

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

Collection and processing of genetic and biometric data for the purpose of health and life insurance is prohibited.

Subject to the above, where processing of genetic and biometric data is based on consent, subsequent and separate consents should be obtained for any further processing.

Further, according to the Law, impact assessment and prior consultation with the Commissioner are required in the following instances:

- when a combination of filing systems of public authorities or certification bodies, is conducted in relation to special categories of personal data or data relating to criminal offences or penalties or will be carried out on the basis of the use of an ID number or any other identifier of general application;
- where, subject to the provisions of Article 23 of the GDPR, measures are taken by the data controller to restrict the rights referred to under Article 12, 18, 19 and 20 of the GDPR;
- where the data controller is exempted from the obligation to notify data subjects for breaches of personal data for one or more of the purposes listed in Article 23(1) of the GDPR, including inter alia, national security, defense, public security, prevention, investigation, detection or prosecution of criminal offences etc;
- where national legislation or regulations issued pursuant thereto provide for a specific action or series of processing activities; and
- where special categories of personal data will be transferred in a third country or an international organization by the controller or the processor, on the basis of a derogation for specific situations provided for under Article 49 of the GDPR.

TRANSFER

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

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

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

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

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

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

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

With regards to transfer of special categories of personal data, prior to such data being transferred to a third country or an international organization on the basis of appropriate safeguards provided for under Article 46 of the GDPR or on the basis of binding corporate rules under Article 47 of the GDPR, the data controller or the processor needs to inform the Commissioner of its intention in transferring the said data. The Commissioner may impose express restrictions for such transfer.

Similarly, when special categories of personal data are to be transferred to a third country or an international organization on the basis of a derogation for specific situations provided for under Article 49 of the GDPR, an impact assessment is required to be carried out as well as prior consultation with the Commissioner and the Commissioner may, for important reasons of public interest, impose express restrictions for such transfer.

In light of the Schrems II decision, the European Data Protection Board (EDPB) has issued Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, in respect of transfers made under the standard contractual clauses. The Commissioner directs organisations to the EDPB Recommendations 01/2020 and urges them to follow the guidance of the EDPB.

For more information, please visit our [Transfer - global data transfer methodology website](#).

SECURITY

Security

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

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

- a. the pseudonymization and encryption of personal data;
- b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

There are no derogations or additional requirements introduced by the Law in relation to security.

BREACH NOTIFICATION

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

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

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

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

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

According to the Law, the data controller may be exempted, in whole or in part, from his obligation to notify data subjects for breaches of personal data for one or more of the purposes listed in Article 23(1) of the GDPR, including *inter*

alia, national security, defense, public security, prevention, investigation, detection or prosecution of criminal offences etc. In order for the foregoing to apply, an impact assessment and a prior consultation with the Commissioner need to be conducted. The Commissioner may also set out specific terms and conditions for such exemption.

ENFORCEMENT

Fines

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

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

Fines are split into two broad categories.

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

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

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

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

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

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

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

Right to claim compensation

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

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

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

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

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

According to the Law, the Council of Ministers may, upon a recommendation of the Commissioner, issue regulatory administrative acts (secondary legislation) in order to effectively enforce the GDPR and applicable national law.

Further, the Law provides that the Commissioner for the Protection of Personal Data shall impose administrative fines in accordance with Article 83 of the GDPR. Further, the Law provides that an administrative fine imposed to a public authority or body, which relates to non-profitable activities shall not exceed EUR 200,000.

The Law provides, inter alia, that breaches of, inter alia, Articles 30, 31, 33, 34, 35, 42 and of Chapter V of the GDPR, shall constitute a criminal offence which may result in the imposition of imprisonment up to three years and / or monetary fine up to EUR 30,000 or imprisonment up to five years and / or monetary fine up to EUR 50,000, depending on the breach.

Where the data controller or processor is a company or a group of undertakings, then the person indicated as such in its article of association will be held liable for breaches of the GDPR and / or the national law. In case of public authorities or bodies, the head of such authority or the person who is effectively exercising the administration of such authority will be held liable for such breaches.

ELECTRONIC MARKETING

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

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

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

The Regulation of Electronic Communications and Postal Services Law of 2004 (I 12(I)/2004) as amended (the "**Electronic Communications and Postal Services Law**") will apply to most electronic marketing activities, as there is likely to be

processing and use of personal data involved (eg, an email address is likely to be personal data for the purposes of the Electronic Communication and Postal Services Law).

Section 106 of the Electronic Communications and Postal Services Law states the following:

1. The use of automatic calling machines, fax, or electronic mail, or SMS messages, for the purposes of direct marketing, may only be allowed in respect to subscribers or users who have given their prior consent
2. Unsolicited communications for the purposes of direct marketing, by means other than those referred to in (1) above, are not allowed without the consent of the subscribers or users concerned
3. The rights referred to in (1) and (2) above shall apply to subscribers who are natural persons. The Commissioner of Electronic Communications and Postal Regulation, may, after consultation with the Personal Data Commissioner, issue orders to safeguard that legitimate interests of legal persons, regarding unsolicited communications, are adequately protected. In 2005, the Commissioner of Electronic Communications and Postal Regulation issued the 2005 Order regarding Safeguarding the Interests of Legal Persons in relation to Unsolicited Communications, by virtue of which the protection from unsolicited communications for the purposes of direct marketing has been extended to legal persons as well
4. Notwithstanding (1) above, in cases where a natural or legal person obtains from its customers contact details for electronic mail, in the context of the sale of a product or a service, the same natural or legal person may use these electronic details for direct marketing of its own similar products or services, provided that customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of their electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use, and
5. Electronic mail sent for direct marketing must not disguise or conceal the identity of the sender or the person on whose behalf and / or for the benefit of the communication is made, or without a valid address to which the recipient may send a request that such communication cease.

ONLINE PRIVACY

Part 14 of the Electronic Communications and Postal Services Law deals with the collection of location and traffic data and use of cookies (and similar technologies) by publically available electronic communication service providers.

Traffic Data

Traffic Data concerning subscribers and users, which are submitted to processing so as to establish communications and which are stored by persons, shall be erased or made anonymous at the end of a call, except:

- for the purpose of subscriber billing and interconnection payments, and
- if the subscriber or user consent that the data may be processed from a person for the purpose of commercial promotion of the services of electronic communications of the latter or for the provision of added value services. Users or subscribers have the possibility to withdraw their consent for the processing of Traffic Data at any time.

The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information. Users or subscribers shall be given the possibility to withdraw their consent for the processing of Traffic Data at any time.

Location Data

Location Data may only be processed when made anonymous, or with the explicit consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.

The service provider must inform the users or subscribers, prior to obtaining their consent, of the following:

- type of Location Data which will be processed
- the purpose and duration of the processing, and
- whether the data will be transmitted to a third party for the purpose of providing the value added service.

Users or subscribers shall be given the possibility to withdraw their consent for the processing of Location Data at any time.

Cookie Compliance

The storage and use of cookies and similar technologies is permitted only if the subscriber or user concerned has been provided with clear and comprehensive information, inter alia, about the purposes of the processing, and has given his consent in accordance with the Processing of Personal Data Law.

The above shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

With regards to information society services, when such services are addressed to a child and provided to him / her on the basis of his / her consent – such consent is valid if he / she is at least 14 years old.

KEY CONTACTS

Pamboridis LLC

www.pamboridis.com/



Christy Spyrou

Partner

T +357 22 752525

spyrou@pamboridis.com

DATA PRIVACY TOOL

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

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.