DATA PROTECTION LAWS OF THE WORLD

Greece

Downloaded: 18 May 2024

GREECE

Last modified 19 January 2024

LAW

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

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

Territorial Scope

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

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

The Greek Law 4624/2019 “on the Hellenic Data Protection Authority, the implementation of Regulation 2016/679 and the transposition of Directive 2016/680” (hereinafter the “Law”) (Government Gazette A/137/29.08.2019) was enacted and entered into force in August 28, 2019. The Law regulates the operation of the Hellenic Data Protection Authority, introduces GDPR supplementary rules and transposes the Law Enforcement Directive into Greek Law.

DEFINITIONS

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

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

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

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

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

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

Definition of supervisory authority

The competent supervisory authority for the territory of Greece is the Hellenic Data Protection Authority (hereinafter the “**HDPA**”).

Definitions as per article 4 of the GDPR

Further to the definitions as per article 4 of the GDPR, the Law provides for specific definitions for the notions of public and private bodies:

- ‘Public body’ means public authorities, independent and regulatory administrative authorities, legal persons governed by public law, first and second-level local government authorities with their legal persons and their legal entities, state-owned or public undertakings and agencies, legal persons governed by private law which are state-owned or regularly receive at least 50% of their annual budget in the form of state subsidies, or their administration is designated by the state;

- ‘Private body’ means any natural or legal person or group of persons without legal personality which does not fall within the definition of a ‘public body’.

Further, as per Law 4961/2022 on “Emerging information and communication technologies, strengthening digital governance and other provisions” the following definitions are worth noting, to the extent related to the data protection regime:

- “Internet of Things” (“IoT”) constitutes any technology that (a) allows devices or a group of interconnected or related devices, through their internet connection, to perform automatic processing of digital data; and (b) enables the collection and exchange of digital data, in order to offer a variety of services to users, with or without human participation.
- “Distributed ledger” is defined as the repository of information that keeps records of transactions, and which is shared and synchronized between a set of DLT network nodes, using a consensus mechanism.
- “Blockchain” is defined as a type of distributed ledger technology that records data in blocks, which are connected to each other in chronological order and form a chain of a consensual, decentralized and mathematically verifiable nature, which is mainly based on the science of cryptography.
- A “smart contract” is defined as a set of coded computer functions, which is finalized and executed through distributed ledger technology in automated electronic form through instructions for the execution of actions, omissions or tolerances, which are based on the existence or not of specific conditions, according to terms recorded directly in electronic code, scheduled commands or programmed language.

NATIONAL DATA PROTECTION AUTHORITY

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

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

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

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

Hellenic Data Protection Authority (HDPA)

Kifissias 1-3
115 23 Athens
Greece

T: +30-210 6475600

F: +30-210 6475628

Email: contact@dpa.gr

The HDPA is responsible for supervising the implementation and enforcement of data protection Law in Greece.

REGISTRATION

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

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

There are no registration requirements under Greek Law. Notification and authorization requirements under the former data protection regime pertaining to the processing of special category data or installation of CCTV systems have been abolished and replaced by the obligation to hold a record of processing activities and to conduct DPIAs.

DATA PROTECTION OFFICERS

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

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

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

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

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

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

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

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

Further to the relevant GDPR provisions, the Law lays down specific rules on the appointment of DPO by public authorities. The particularity of Greek law is that public authorities can be considered to be exempted from the obligation to publish the contact details of the DPO and communicate them to the HDPA for reasons of national security or confidentiality.

COLLECTION & PROCESSING

Data Protection Principles

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

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

- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

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

Legal Basis under Article 6

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

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

Special Category Data

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

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

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

Criminal Convictions and Offences data

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

Processing for a Secondary Purpose

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

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

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

Transparency (Privacy Notices)

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

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

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

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

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

Rights of the Data Subject

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

Right of access (Article 15)

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

Right to rectify (Article 16)

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

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

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

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

Right to restriction of processing (Article 18)

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

Right to data portability (Article 20)

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

Right to object (Article 21)

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

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

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

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

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

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

- The Law establishes additional purposes in relation to which further processing is allowed.

- With regard to public bodies, processing of personal data for a purpose other than that for which they were collected shall be permitted where such processing is necessary for the performance of the tasks assigned to them and provided that it is necessary:
    - for the verification of the information provided by the data subject because there are reasonable grounds for believing that such information is incorrect;
    - for the prevention of risks to national security, defense or public security, or for securing tax and customs revenue;
    - for the prosecution of criminal offences;
    - for the prevention of serious harm to the rights of another person;
    - for the production of official statistics.

- With regard to private bodies, processing of personal data by private bodies for a purpose other than that for which they have been collected shall be permitted, where necessary:
    - for the prevention of threats to national or public security at the request of a public body; or
    - for the prosecution of criminal offences; or
    - for the establishment, exercise or defense of legal claims, unless the interests of the data subject override the grounds for the processing of those data.

- Data Processing in the Employment context: Βy virtue of the right conferred by Article 88 of the GDPR, the Law lays down detailed sector specific rules in respect for data processing in the context of the employment relationship.

Employee’s personal data can be processed for purposes related to recruitment or the performance of the employment agreement.

Processing of special categories of personal data for employment-related purposes is allowed (i) if necessary to exercise rights or comply with legal obligations derived from labor law or social security and social protection law and (ii) the data controller has no reason to believe that the data subject has an overriding legitimate interest.

Data processing may only exceptionally be based on employee’s consent. Consent may be considered as informed, if the employer has informed the employee about the processing purpose and the right to revoke his / her consent. To assess whether consent is freely given due attention should be paid to the level of dependency of the employee and the conditions under which consent was granted. Consent can be given also by electronic means and should not be tied to the employment agreement. Consent to processing of specific categories of data should be given in relation to said data.

The processing of personal data is also permitted on the basis of collective labor agreements.

Data controllers must take appropriate measures to ensure compliance with the processing principles set forth in Article 5 of the GDPR when processing employees’ data.

Video Surveillance by means of CCTV systems in the workplace is permitted only for reasons of safety and security, provided that employees have been previously informed thereabout. Such data cannot be used for evaluation purposes.

Processing sensitive personal data / consent

- Collection and processing of genetic data for health and life insurance purposes is prohibited under Article 23 of the Law.

- By way of derogation from Article 9 para. 1 of the GDPR, the processing of special categories of personal data within the meaning of Article 9 para. 1 of the GDPR by public and private bodies shall be allowed, if necessary: (a) for the purpose of exercising the rights arising from the right to social security and social protection, and for fulfilling the obligations arising therefrom; (b) for the purposes of preventive medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or the management of health or social care systems or pursuant to a contract with a health professional or other person who is subject to a duty of professional secrecy or supervised by him/her; or (c) for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, in addition to the measures referred to in the second subparagraph of paragraph 3, the provisions ensuring professional secrecy provided for in a law or code of conduct must in particular be complied with. It goes without saying that the processing of special categories of personal data shall be accompanied by the implementation of the appropriate technical and organisational measures.

- By way of derogation from Article 9 para. 1 of the GDPR, the processing of special categories of personal data by public bodies within the meaning of Article 9 para. 1 of the GDPR shall be allowed, where it is: (a) strictly necessary for reasons of essential public interest; (b) necessary for the prevention of major threats to national or public security; or (c) necessary for taking humanitarian action, in which case the interests in the processing override the interests of the data subject.

Further Processing

- With regard, in particular, to public bodies, the processing of special categories of personal data, as referred to in Article 9 para. 1 of the GDPR, for a purpose other than that for which they have been collected, shall be permitted provided that the conditions set out in the paragraph 1 of Art. 24 of Law 4624/2019 are fulfilled and one of the exemptions provided for in Article 9 para. 2 of the GDPR or Article 22 of Law 4624/2019 applies.

  As far as private bodies is concerned, the processing of special categories of personal data, as referred to in Article 9 para. 1 of the GDPR, for a purpose other than that for which they have been collected, shall be permitted, provided that the conditions set out in the paragraph 1 of Art. 25 of Law 4624/2019 are fulfilled and one of the exemptions provided for in Article 9 para. 2 of the GDPR or Article 22 of Law 4624/2019 applies.

- **Processing and Freedom of Expression and Information:** Exercising the discretion under Article 85 GDPR, the Law sets the conditions for data processing that is necessary to uphold the right to freedom of expression and information and precludes in this case the application of the majority of data controller’s obligations.

  To the extent necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression, the processing of personal data is allowed where: (a) the data subject has given his or her explicit consent, (b) it relates to personal data which are manifestly made public by the data subject, (c) the right to freedom of expression and the right to information override the right to the protection of the data subject’s personal data, in particular on matters of general interest or where it relates to personal data of public figures, and (d) where it is limited to what is necessary to ensure freedom of expression and the right to information, in particular with regard to special categories of personal data, criminal proceedings, convictions and related security measures, taking into account the right of the data subject to his or her private and family life.

  To the extent necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression, the following shall not apply: (a) Chapter II of the GDPR (principles), except for Article 5, (b) Chapter III of the GDPR (rights of the data subject), c) Chapter IV of the GDPR (controller and processor), except for Articles 28, 29 and 32, (d) Chapter V of the GDPR (transfer of personal data to third countries or international organisations), (e) Chapter VII of the GDPR (cooperation and consistency) and f) Chapter IX of the GDPR (specific data processing situations)” (Article 28 para. 2 of Law 4624/2019).

- **Processing for Archiving, Scientific or Historical Research or Statistical Purposes:** Having regard to the margin of discretion under Article 89 of the GDPR, the Law stipulates the security requirements for processing data for archiving, scientific or historical research or statistical purposes and restricts the scope of data subject’s rights.

  1. By way of derogation from Article 9 para. 1 of the GDPR, special categories of personal data within the meaning of Article 9 para. 1 of the GDPR shall be processed where it is necessary for archiving purposes in the public interest. The controller shall have the obligation to take suitable and specific measures to protect the data subject's legitimate interests.

  In derogation from the provisions of Article 15 of the GDPR the access right of the data subject can be restricted in whole or in part to data related to it, if exercise of the right could possibly hinder the fulfillment of archiving purposes in the public interest (as provided in Art. 29 para. 1 of Law 4624/2019), especially in the case that the archiving material is not kept in relation to the data subject's name and the exercise of the right would require disproportionate efforts (Article 29 para. 2 of Law 4624/2019).

  In derogation from the provisions of Article 16 of the GDPR the data subject does not have the right of rectification of inaccurate data, if its exercise could possibly hinder the fulfillment of archiving purposes in the public interest or the exercise of third parties’ rights (Article 29 para. 3 of Law 4624/2019).

  In derogation from the provisions of Articles 18 para. 1 (a) (b) and (d), 20 and 21 of the GDPR, the data subject’s rights shall be restricted, if these rights could possibly hinder the fulfillment of the specific archiving purposes in the public interest (as provided in Art. 29 para. 1 of Law 4624/2019) and such limitations are considered as necessary for the fulfillment of those purposes (Article 29 para. 4 of Law 4624/2019).

  2. By way of derogation from Article 9 para. 1 of the GDPR, the processing of special categories of personal data, within the meaning of Article 9 para. 1 of the GDPR, shall be allowed without the consent of the data subject where the processing is necessary for scientific or historical research purposes, or for the collection and maintenance of statistical information, and the interest of the controller is overriding the interest of the data subject in not having his or her personal data processed. The controller shall have the obligation to take suitable and specific measures to protect the data subject's legitimate interests.

  By way of derogation form the provisions of Articles 15, 16, 18 and 21 of the GDPR, the rights of the data subject shall be limited where their exercise is likely to render impossible or seriously impair the achievement of the objectives referred to in paragraph 1 and where such limitations are deemed to be necessary for their achievement. For the same reason, the data subject’s right of access provided for in Article 15 of the GDPR shall not apply where personal data are necessary for scientific purposes and the provision of information would entail a disproportionate effort (Article 30 para. 2 of Law 4624/2019).

  In addition to what is referred to in paragraph 1, special categories of personal data, where processed for the purposes of paragraph 1 shall, unless it is contrary to the legitimate interest of the data subject, be anonymised as soon as the scientific or statistical purposes allow. Until then, the characteristics that can be used to match individual details associated with personal or real situations of an identified or identifiable person must be stored separately. These characteristics can only be combined with individual details if required for research or statistical purposes (Article 30 para. 3 of Law 4624/2019).

  The controller may publish personal data processed in the context of research, if the data subjects have given their consent in writing or the publication is necessary for the presentation of the results of the research. In the latter case, the results shall undergo pseudonymisation prior to being published (Article 30 para. 4 of Law 4624 /2019).

Confidentiality and data protection measures as regards Whistleblowing channels

Any processing activity conducted on data collected from whistleblowers shall be carried out in accordance with the GDPR and Law 4624/2019, and shall rely on the legal basis of ensuring compliance with a legal obligation to which the controller is subject (Article 6 (1)(c) of the GDPR), in this case being the establishment of reporting channels and the implementation of the measures necessary for the monitoring of those channels.

Further, companies shall implement the appropriate technical and organizational measures, such as pseudonymisation measures, both at the time of report follow-ups as well as during communication with the competent authorities.

TRANSFER

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

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

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

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

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

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

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

Τhe Law does not provide for any additional rules on cross-border data transfers.

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

SECURITY

Security

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

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

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

Greek Law does not provide for additional requirements in relation to security measures other than those set forth in the GDPR. Only with regard to special categories of data, the Law provides an indicative list of the security measures, which should be taken. More specifically, when processing special categories of personal data, appropriate security measures to safeguard the data subject’s interests should be adopted. Such measures may include:

- Technical and organizational measures to ensure that processing complies with the GDPR.
- Measures to verify and establish whether and by which party personal data were fed into, altered or removed.
- Data Protection awareness
- Data classification and access rights
- Designation of a DPO
- Pseudonymization of personal data
- Encryption of personal data
- Measures to restore confidentiality, integrity, availability and resilience of processing systems and services, including the ability to restore availability and access to data in the event of physical or technical incident
- Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

BREACH NOTIFICATION

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

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

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

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

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

The Law does not derogate from the provisions of the GDPR.

It is worth noting, however, that it provides for an additional exception from the obligation to communicate data breaches to the data subject under Article 34 GDPR. Article 33 (5) of the Law provides that in addition to the exception established in Article 34 (3) GDPR, the obligation to communicate a personal data breach to the data subject does not apply when such notification would lead to disclosure of information which must be kept confidential by operation of law or due to their nature, unless the data subject’s interests take precedence.

Further, according to the Hellenic Data Protection Authority (“**HDPA**”), the procedure to be followed for a Data Breach Notification is the following:

- The Controller may complete the relevant form and submit it to the HDPA electronically via its web portal;
- By way of exception, as regards entities that are not established in Greece, the notification of the data breach procedure may be made via email.

ENFORCEMENT

Fines

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

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

Fines are split into two broad categories.

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

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;

- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

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

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

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

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

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

Right to claim compensation

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

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

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

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

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

Administrative fines

The HDPA may impose administrative fines in accordance with article 83 para. 4 and 5 of the GDPR. The acts of the DPA through which administrative fines are imposed, constitute enforceable deeds and shall be served to the data controller, the data processor or their representatives. Such fines shall be collected according to the Public Income Collection Code.

It is worth noting that the largest fine issued to date by the HDPA amounts to EUR 20 million whilst the total value of all fines issued to date amounts to over EUR 32 million.

Penalties

In exercise of the discretionary powers recognized to Member States by Article 84 of the GDPR, the Law stipulates criminal sanctions which may be applied for unauthorized processing:

- Any act of unauthorized data processing (i.e. access, disclosure, destruction or damage collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction) may lead to imprisonment of up to 1 year.
- If the above mentioned actions relate to special categories of data or data relating to criminal convictions, and offences or related security measures, they are punishable by imprisonment of up to 1 year and penalty payment up to 100.000€. Any person who commits the above actions with intent to obtain unlawful advantage or to cause injury amounting to at least 120.000€, is liable to imprisonment of up to 10 years.
- In the event that the above actions threaten democracy or national security, punishment of imprisonment and penalty payment of up to 300.000€ may be applied.

Right to claim compensation

Further to Article 79 (2) of the GDPR, the Law establishes procedural rules with regard to the venue where civil proceedings may be initiated. Claims for damages brought by data subjects against data controllers or processors as a result of a GDPR infringement shall be filed before the civil court of the registered seat of the controller / processor or the court in whose district the data subject has his / her habitual residence.

ELECTRONIC MARKETING

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

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

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

Electronic marketing is regulated by Law 3471/2006 ‘for the protection of personal data and privacy in electronic communications’ (the 'Law’), in combination with the general provisions of Law 2472/1997 *‘for the protection of individuals from the processing of personal data’* (the 'Data Protection Act’).

According to the provisions of article 11 of the Law, data processing for electronic marketing purposes is allowed only upon the individuals’ prior express consent. The said article prohibits the use of automated calling systems for marketing purposes to subscribers that have previously declared to the public electronic communications services providers ('CSPs') that they do not wish to receive such calls in general. The CSPs must register these declarations for free on a separate publicly accessible list.

Personal data (such as e-mail addresses) that have been legally obtained in the course of sales of products, provision of services or any other transaction may be used for electronic marketing purposes, without the receiver’s prior consent thereto, provided that the receiver of such email has the possibility to 'opt out' for free to the collection and processing of his/ her personal data for the aforementioned purposes.

Direct marketing emails or advertising emails of any kind are absolutely prohibited, when the identity of the sender is disguised or concealed and also when no valid address, to which the receivers can address requests for the termination of such communications, is provided.

Electronic marketing is regulated by Greek Law 3471/2006 ‘for the protection of personal data and privacy in electronic communications’, which transposes Directive 2002/85/EC into Greek Law, in conjunction with the GDPR.

According to the provisions of article 11 of Greek Law 3471/2006, data processing for electronic marketing purposes is allowed only upon the individuals’ express prior consent. Use of automated calling systems without human intervention for marketing purposes is prohibited in respect of subscribers that have declared to the public electronic communication services providers ('CSPs') that they do not wish to receive such calls.

Where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services, without prior consent, provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

ONLINE PRIVACY

Articles 4 and 6 of the Law (as amended by Directive 2009/136/EC) deals with the collection of location and traffic data by CSPs and the use of cookies and similar technologies.

Traffic data

Traffic data of subscribers or users held by a CSP must be erased or anonymized after the termination of a communication, unless they are retained for one the following reasons:

- The billing of subscribers and the payment of interconnections, provided that the subscribers are informed of the categories of traffic data that are being processed and the duration of processing, which must not exceed 12 months from the date of the communication (unless the bill is doubtable or unpaid).

- Marketing of electronic communications services or value added services, to the extent that traffic data processing is absolutely necessary and following the subscriber’s or the user’s prior express consent thereto, after his / her notification regarding the categories of traffic data that are being processed and the duration of the processing. Such consent may be freely recalled. The provision of electronic communication services by the CSP must not depend on the subscriber’s consent to the processing of his/her traffic data for other purposes (*eg,* marketing purposes).

Location data

Location data may only be processed for the provision of value added services, only if such data are anonymized or with the subscriber’s / user’s express consent, to the extent and for the duration for which such processing is absolutely necessary. The CSP must previously notify the user or the subscriber of the categories of location data that are being processed, the purposes and the duration of the processing as well as of the third parties to which the data will be transmitted for value added services provision. The subscriber’s / user’s consent may be freely recalled and the 'opt-out' possibility must be provided to the subscriber by the CSP free of charge and with simple means, every time he is connected to the network or in each transmission of communication.

Location data processing is allowed exceptionally without the subscriber’s / user’s prior consent to authorities dealing with emergencies, such as prosecution authorities, first aid or fire-brigade authorities, when the location of the caller is necessary for serving such emergency purposes.

Cookie compliance

The use and storage of cookies and similar technologies is allowed when the subscriber / user has provided his express consent, after his / her comprehensive and detailed notification by the CSP. The subscriber’s consent may be provided through the necessary browser adjustments or through the use of other applications.

The latter do not prevent the technical storage or use of cookies for purposes relating exclusively to the transmission of a communication through an electronic communications network or the provision of an information society service for which the subscriber or the user has specifically requested. The Data Protection Authority is the competent authority for the issuance of an Act, which will regulate the ways such services will be provided and the subscribers’ consent will be declared.

Articles 4 and 6 of Greek Law 3471/2006 regulate collection of location and traffic data by CSPs and the use of cookies and similar technologies.

Traffic data

Traffic data held by a CSP must be in principle erased or anonymized upon termination of the communication to which they refer. The aforementioned rule does not apply with regard to traffic data retained for billing, marketing and law enforcement purposes.

Location data

Location data may only be processed for the provision of value added services, only if they are anonymized or upon subscriber’s / user’s express consent, unless processing and disclosure of such data to public authorities is necessary in case of emergency.

Cookies compliance

Rules on use of cookies and similar technologies are set forth in the HDPA Guidance Note on “the use of cookies and other tracking technologies”. The use and storage of cookies and similar technologies is allowed when the subscriber / user has provided his express consent. The subscriber’s consent may be provided by means of cookie pop-up or banners and shall meet GDPR consent requirements.

Use of cookies for purposes relating exclusively to the transmission of a communication through an electronic communications network or the provision of an information society service for which the subscriber or the user has specifically requested, are exempted from aforementioned requirement.

KEY CONTACTS

Kyriakides Georgopoulos Law Firm
www.kglawfirm.gr

Irene C. Kyriakides
Partner
Kyriakides Georgopoulos Law Firm
i.kyriakides@kglawfirm.gr

DATA PRIVACY TOOL

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

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.