GREECE

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.

DEFINITIONS

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

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

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

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

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

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

**Definition of supervisory authority**

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

**Definitions as per article 4 of the GDPR**

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

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

**NATIONAL DATA PROTECTION AUTHORITY**

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

The GDPR creates the concept of "lead supervisory authority". Where there is cross-border processing of personal data (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.
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 is no requirement in the Bill to notify/register with the DPA.

DATA PROTECTION OFFICERS

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

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

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

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

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

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

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities,
This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

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

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

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

**COLLECTION & PROCESSING**

**Data Protection Principles**

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

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

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. 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 - i.e., use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

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

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

**Transparency (Privacy Notices)**

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

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

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

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

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

**Rights of the Data Subject**

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

**Right of access (Article 15)**

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

**Right to rectify (Article 16)**

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

**Right to erasure (‘right to be forgotten’) (Article 17)**

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

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

**Right to restriction of processing (Article 18)**

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

**Right to data portability (Article 20)**

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

**Right to object (Article 21)**

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

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

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

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

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

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

**Processing personal data**

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

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

- Processing of personal data in the context of employment from an employer as data controller is allowed as long as:
  - it is necessary for the fulfillment of respective obligations related to the employment contract or deriving from the law or an individual or collective employment contract
In the case that the data collection and processing is based on the consent of employees, such consent shall be written and distinguished from the employment contract. The employee shall have given his free and explicit consent and have the right to deny or withdraw his consent without negative impacts.

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

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

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

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

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

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

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

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

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

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

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

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

In derogation from the provisions of Article 15 of the GDPR the access right of the data subject can be restricted in whole or in part to data related to it, if exercise of the right could possibly hinder the fulfillment of archiving purposes in the public interest, especially in the case that the archiving material is not kept in relation to the data subject’s name and the exercise of the right would require disproportionate efforts.

In derogation from the provisions of Article 16 of the GDPR the data subject does not have the right of rectification of inaccurate data, if the exercise of this right could possibly hinder the fulfillment of archiving purposes in the public interest or the exercise of third parties’ rights.

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

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

**Processing sensitive personal data / consent**

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

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

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

- Processing of personal data relating to criminal convictions and offences is permitted, if it is strictly necessary for the purpose of one of the following:
  - Recruitment and assessment for job positions
  - Employment relations under the certain preconditions and guarantees of article 17
Archiving in the public interest, scientific or historical research or statistics in accordance with articles 18 and 19
Academic, artistic, literary and journalistic expression in the scope of freedom of expression and information
Establishment, exercise and defense of legal claims

Processing of personal data relating to criminal convictions and offences is permitted upon the explicit and written consent of the data subject, if it is necessary to take measures requested by the data subject, such as reintegration. Furthermore, the processing of those personal data in the scope of academic, artistic, literary as well as journalistic purposes shall be the adequate, relevant and limited to secure the freedom of expression and the right to information (‘data minimisation’).

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

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

TRANSFER

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

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

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

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

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

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.
Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

The transfer of personal data is permitted:

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

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

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

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

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

**SECURITY**

**Security**

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

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

a. the pseudonymization and encryption of personal data;

b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

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

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

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

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

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

**BREACH NOTIFICATION**

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

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

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

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the 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.

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

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

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

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

- national security
- national defense
- public security
- prevention, investigation or prosecution of criminal convictions and offences, including the protection from and prevention of threats against public security
- important economic or financial state interests including monetary, financial and tax, public health as well as social insurance issues, especially regarding performance of relevant audits
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 DPA may impose administrative fines in accordance with article 83 para. 4 and 5 of the GDPR. The acts of the DPA through which administrative fines are imposed, constitute enforceable deeds and shall be served to the data controller, the data processor or their representatives. Such fines shall be collected according to the Public Income Collection Code.

### Penalties

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

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

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

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

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

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

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

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

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

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

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. 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.
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.

**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.

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 doubtful or unpaid).

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

Location data

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

KEY CONTACTS

Kyriakides Georgopoulos Law Firm

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 © 2017 DLA Piper. All rights reserved.