Contents

Global Privacy and Security Law - Gilbert, GREECE by George Ballas, Zoe Provata, and Nikolaos Papadopoulos

Global Privacy and Security Law - Gilbert
Global Privacy and Security Law - Gilbert
GREECE by George Ballas, Zoe Provata, and Nikolaos Papadopoulos

Click to open document in a browser

Global Privacy and Security Law - Gilbert, § GRC.00, Greece,COUNTRY OVERVIEW

Francoise Gilbert, Global Privacy and Security Law § GRC.00 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

Capital	*Athens*
Official Language	*Greek*
Political System	*Parliamentary Republic*
Population	*10.4 million*
Currency	*Euro*
Entry in the European Union	*1981*

[A] Location

Located near the crossroads of Europe and Asia, Greece, or the Hellenic Republic, forms the southern extremity of the Balkan Peninsula in southeast Europe. It borders Albania, Bulgaria, North Macedonia, and Turkey. The country has more than 2,000 island territories and only about 227 of them are inhabited.

The country is divided into 13 administrative regions: Attica, Central Greece, Central Macedonia, Crete, Eastern Macedonia and Thrace, Epirus, Ionian Islands, North Aegean, Peloponnese, South Aegean, Thessaly, Western Greece, Western Macedonia, and Monastic Communities of Mount Athos.

[B] Constitution and Government

Modern Greece has a republican structure based on the constitution of 1975. The constitution has been amended several times since then, in 1986, 2001, 2008, and 2019. The Constitutional Amendment of 1986 redefined the presidential duties and powers.

The Constitution consists of 120 articles, and provides for separation of powers into executive, legislative, and judicial branches. The Constitution grants special guaranties of civil liberties and social rights.

[C] Executive Branch

The President of the Hellenic Republic is the head of state and is elected by Parliament for a five-year term. The Prime Minister is the head of Government. The position is filled by the current leader of the political party that holds the majority of seats in the Parliament, or that can obtain a vote of confidence from the Parliament. The President of the Republic formally appoints the Prime Minister.

The Cabinet is appointed by the President on recommendation of the Prime Minister. The President also dismisses the Cabinet on recommendation of the Prime Minister.

[D] Legislative Branch

Greece has a single-chamber parliament consisting of 300 members, who are elected for a period of four years. The statutes that are passed by the Parliament are promulgated by the President of the Republic.

[E] Judicial Branch

The Judicial Branch is divided into two main jurisdictions:

- The civil and penal jurisdiction which includes the Courts of First Instance, the Courts of Second Instance, and the Supreme Court called “Areios Pagos”; and
- The administrative jurisdiction, which includes the Administrative Courts of First Instance, the Administrative Courts of Second Instance, the Supreme Administrative Court called “the Council of State,” and the Court of Audits which acts as the competent court for certain public accounting issues.

In case of contradictory decisions between the Supreme Courts, the case is referred to the Supreme Special Court.

The Greek judges are selected through a national competition and they are appointed through a Presidential Decree confirming their successful graduation from the National School of Judges. Greek judges explicitly enjoy personal and functional independence and a life tenure, which expires by law at the age of 65 for the judges serving at the Courts of First and Second Instance and at the age of 67 for the Supreme Court Judges.

[F] Legal System

The legal system is based on civil law, which is derived from Roman Law.

[G] Membership in International Organizations

Greece joined the European Union in 1981. It has been a member of the United Nations since 1945, the Council of Europe since 1949, NATO since 1952, the OECD since 1960, and the Organization for Security and Co-operation in Europe (OSCE) since 1973.

[H] Economy

Greece's main economic sectors are agriculture, tourism, construction, and shipping. More than 50% of Greek industry is located in the Greater Athens area. [1]

Footnotes

1 Source for this section: https://europa.eu/european-union/about-eu/countries/member-countries/greece_en.

Global Privacy and Security Law - Gilbert, § GRC.01, Greece,International or Regional Treaties and Agreement

Francoise Gilbert, Global Privacy and Security Law § GRC.01 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

[A] United Nations

Greece is a member of the United Nations. As such, it adheres to the United Nations Universal Declaration of Human Rights. Article 12 of the Declaration of Human Rights states:

> *No one shall be subjected to arbitrary interference with his/her privacy, family, home, or correspondence, nor to attacks upon his/her honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

[B] Organization for Economic Cooperation and Development (OECD)

Greece is a member of the Organization for Economic Cooperation and Development (OECD) and therefore it is expected to follow the guidelines issued by the OECD. In the area of privacy and cybersecurity, the current guidelines and recommendations include:

- Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines) (1980, updated in 2013); [2]
- Guidelines for the Security of Information Systems and Networks (2002), which have been replaced by the Recommendations on Digital Security Risk Management for Economic and Social Prosperity (2015) [3] which were supplemented by OECD Recommendation on Digital Security of Critical Activities in December 2019. [4]

[C] European Union Treaties and Agreements

As part of its membership in the European Union, Greece is subject to the treaties and agreement that are part of the EU framework. This includes, among others, the following:

[1] Treaty on the European Union

Greece is a signatory of the Treaty on European Union. [5] Article 6 of the Treaty on European Union states:

> *Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law .*

[2] Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union [6] is also applicable in Greece. Article 8 (Protection of personal data) of the Charter of fundamental rights states:

> *(1) Everyone has the right to the protection of personal data concerning him or her.*
>
> *(2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> *(3) Compliance with these rules shall be subject to control by an independent authority.*

[D] Council of Europe Conventions

As a member of the Council of Europe (COE), Greece is subject to the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950). It also adheres to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981).

[1] Council of Europe Convention on Human Rights

In 1949, Greece became the eleventh member state of the Council of Europe. As such, it adheres to the Convention for the Protection of Human Rights and Fundamental Freedoms (the "European Convention on Human Rights"). [7] Article 8 (Right to respect for private and family life) of the European Convention on Human Rights states:

> *(1) Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

[2] Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data

Being a member of the Council of Europe, Greece also adheres to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108. [8] Greece has also signed, but not yet ratified, the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No. 181). [9]

In November 2018, the Council of Europe completed its process to update Convention 108 in order to deal with challenges resulting from the use of new information and communication technologies. A protocol amending Convention 108 (Protocol CETS No. 223) was adopted in November 2018. [10] The new updated Convention, known as "Convention 108+" is currently open for signatures. [11] Greece has signed but not yet ratified Protocol CETS No. 223. [12]

Footnotes

2 Text *available at* http://www.oecd.org/intant/ieconomy/privacy-guidelines.htm https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

3 Text *available at* http://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm.

4 Text *available at* http://www.oecd.org/sti/ieconomy/recommendation-on-digital-security-of-critical-activities.htm.

5 Consolidated version of the Treaty on European Union, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012M/TXT.

6 Charter of fundamental rights of the European Union (2000/C 364/01), *available a* t https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

7 European Convention on Human Rights (as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13, and 16), *available at* https://www. echr.coe.int/Documents/Convention_ENG.pdf.

8 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), *available at* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

9 Text *available at* https://rm.coe.int/1680080626.

10 Text *available at* https://rm.coe.int/16808ac918.

11 The text of Convention 108+, which incorporates all of the amendments resulting from Protocol CETS No. 223 is *available at* https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. *See also* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223.

12 From the date of entry into force of Protocol CETS No. 223l, the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181) shall be repealed.

Global Privacy and Security Law - Gilbert, § GRC.02, Greece,CONSTITUTION

Francoise Gilbert, Global Privacy and Security Law § GRC.02 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

The Constitution of Greece recognizes the right to private and family life. [13] Under Article 9, every person's home is a sanctuary; the private and family life of the individual is inviolable. Article 19 recognizes the right to secrecy of communications.

In 2001, the Constitution was amended to provide in Article 9A, the right of protection of an individual's personal data. Article 9A states: " *All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law.* " The 2001 amendment to the Constitution also established an independent authority responsible for ensuring the protection of these rights.

Footnotes

13 Constitution of Greece (1975) as amended in 2008, *available at* https://www. hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156%20 aggliko.pdf.

Global Privacy and Security Law - Gilbert, § GRC.03, Greece,NATIONAL DATA PROTECTION LAW—INTRODUCTION

Francoise Gilbert, Global Privacy and Security Law § GRC.03 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

[A] EU General Data Protection Regulation

On May 25, 2018, the EU General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) entered into force. Because of its structure as a regulation, rather than a directive, the GDPR became de facto the primary data protection law of each Member State of the European Union. Therefore, the GDPR applies in Greece.

The GDPR provides EU Member States with the ability to modify or supplement the base GDPR with provisions that apply only at the member-state level and that are consistent with the current culture and treatment of personal data in the particular Member State. In addition, the GDPR permits sector-specific data protection laws and regulations in each Member State.

[B] Greece-Specific Provisions

In addition to the GDPR, the relevant national data protection laws of Greece include the following:

- **Law 4624/2019** , which has introduced supplemental measures for the application of the GDPR; it has also incorporated Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. [14] Law 4624/ 2019 abolished prior Data Protection Law 2472/1997, with the exception of certain of its provisions which remain in force, e.g., regarding the processing of data by judicial authorities in case of specific offenses, the use of surveillance technologies in public meetings and the opt-out register for commercial communications by post and administrative sanctions in case of breach of e-privacy Law 3471/2006;
- **Law 3471/2006** on the processing of personal data and the protection of privacy in the electronic communications sector, [15] which has transposed Directive (EU) 2002/58/EC; [16]
- **Law 4579/2018** , which has transposed Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation, and prosecution of terrorist offences and serious crime;
- **Law 3783/2009** on the identification of owners and users of equipment and services for mobile telephony; and
- **Law 3917/2011** which has transposed Data Retention Directive 2006/24/EC, applicable to providers of publicly available electronic communication services or of public communication networks.

Footnotes

14 Law 4624/2019 was adopted following the European Commission's decision of 25 July 2019 to refer Greece (and Spain) to the Court of Justice of the European Union (CJEU) for having failed to transpose Directive (EU) 2016/680 on time. The Greek authorities rushed in order to adopt a new data protection law; as a result, and as argued by legal scholars and the Hellenic Data Protection Authority, Law 4624/2019 suffers from important shortcomings, and it has introduced provisions of questionable compliance and compatibility with the GDPR and Directive (EU) 2016/680.

15 EN version, *available at* https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW_%203471_06EN.PDF.

16 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Global Privacy and Security Law - Gilbert, § GRC.04, NATIONAL DATA PROTECTION LAW—DEFINITIONS AND KEY CONCEPTS

Francoise Gilbert, Global Privacy and Security Law § GRC.04 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

The text of the GDPR relies on several key terms. These definitions are found primarily in GDPR Art. 4.

[A] Data Subject

A “data subject” is a natural person, identified or unidentifiable. An identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identifier, such as name, an identification number, location data, and an online identifier or by one or more factors specific to the person's physical, physiological, genetic, mental, economic, cultural, or social identity. [17]

[B] Data to Be Protected

The GDPR defines several types of data related to a data subject.

[1] Personal Data

“Personal data” is defined as any information relating to an identified or identifiable natural person or “data subject.” [18] Data protection legislation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. [19]

[2] Sensitive Data or Special Categories of Data

Several categories of data, generally known as “sensitive data,” receive special protection. These categories of data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data (when used to uniquely identify a natural person), and data concerning health or a person's sex life or sexual orientation. [20]

[3] Personal Data Relating to Criminal Convictions and Offences

Pursuant to Art. 10 of the GDPR, the processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects, while any comprehensive register of criminal convictions shall be kept only under the control of official authority.

[4] Children’s Data

Certain provisions of GDPR provide for increased protection with regard to children personal data. Pursuant to Art. 8 of the GDPR, in relation to the offer of information society services directly to a child, child’s consent for the processing of their personal data is lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.

Member States are permitted to change this age limit to between 13 and 16 years. In Greece, the age threshold is 15. In any other case of processing personal data relating to data subjects below the age of 18 years based on consent, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.

[5] Personal Data of Deceased Persons

Recital 27 of the GDPR Preamble clarifies that GDPR does not apply to the personal data of deceased persons. Sections 158 and 160 of the GDPR Preamble reiterate the statement of Recital 27, specifying that personal data may in some circumstances by used in connection with archiving and for historical research, or genetic analysis,

and that entities conducting this archiving or historical research or research for genealogical purposes should keep in mind that GDPR should not apply to personal data of deceased persons.

Recital 27 of the Preamble also ensures that the general statement about inapplicability of the GDPR to deceased person does not create an obstacle for Member States that may have different preferences. Recital 27 of the GPDR Preamble allows Member States to provide for rules regarding the processing of personal data of deceased persons.

[6] Pseudonymized Data

GDPR Art. 4(5) defines “pseudonymization” as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

[7] Anonymized Data

Section 26 of the GDPR Preamble states that the principles of data protection do not apply to anonymous information, which it defines as information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

[C] Data Controllers and Processors

[1] Data Controller

Under the GDPR, a “controller” is a natural or legal person, public authority, agency, or other body that alone or jointly with others determines the purposes and means of the processing of personal data. [21]

There is no additional provision in Greek law.

[2] Data Processor

The GDPR defines a “processor” as a natural or legal person, public authority, agency, or another body that processes personal data on behalf of a data controller. [22]

[D] Data Protection Officer

In some circumstances, the GDPR requires data controllers and processors to appoint a “data protection officer (DPO).” [23] The DPO is responsible for informing and advising the data controller or the data processor and any employees who are processing personal data of their obligations under GDPR and for monitoring compliance with GDPR.

[E] Key Government Entities

Several entities have a significant role in the application and implementation of the GDPR. These include:

[1] Supervisory Authority

In each Member State, the activities of data controllers and data processors are overseen by one or more supervisory authorities. [24] Each Member State must have one or more independent public authorities responsible for monitoring the application of the GDPR, protecting the fundamental rights and freedoms of individuals in relation to the processing of their personal data, and facilitating the free flow of personal data within the EU/EEA. [25]

In Greece, it is the *Hellenic Data Protection Authority* , a constitutionally consolidated independent authority, which monitors compliance and enforces the applicable data protection legislation.

[2] European Data Protection Supervisor (EDPS)

The European Data Protection Supervisor (EDPS) is an independent supervisory authority whose primary role is to ensure that European institutions and bodies respect the right to privacy and data protection when they process personal data and develop new policies. The nature, role, and authority of the EDPS are defined in Regulation (EU) 2018/1725, which repealed Regulation (EC) No. 45/2001 (2001).

[3] European Data Protection Board (EDPB)

The European Data Protection Board (EDPB) is an independent European body that contributes to the consistent application of data protection rules throughout the European Union and promotes cooperation between the EU's data protection authorities. The EDPB is established by the GDPR. The EDPB is composed of the head of one supervisory authority of each EU Member State and of the European Data Protection Supervisor (EDPS), or their respective representatives. [26]

Footnotes

17 GDPR Art. 4(1).

18 GDPR Art. 4(1).

19 GDPR Art. 2(2c), Recital (18). Also, the Hellenic Data Protection Authority ruled with Decision 22/2022 that the GDPR does not apply in the case of the installation and operation of cameras inside the rooms of a household, because the processing of personal data falls within the "exclusively personal and domestic activity" exception, regardless of the fact that the complainant was obliged to go to the other party's home in order to exercise the right to communicate with his child in the presence of the other party.

20 GDPR Art. 9(1).

21 GDPR Art. 4(7).

22 GDPR Art. 4(8).

23 GDPR Arts. 37 to 39.

24 GDPR Art. 51.

25 GDPR Art. 51.

26 GDPR Art. 68.

Global Privacy and Security Law - Gilbert, § GRC.05, Greece,NATIONAL DATA PROTECTION LAW—TERRITORIAL SCOPE

Francoise Gilbert, Global Privacy and Security Law § GRC.05 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

The GDPR applies to entities established in a Member State and, in certain circumstances, to entities that are established elsewhere and process personal data of individuals who are in a Member State.

[A] Entities Established in the EU

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a data controller or a data processor in the EU, whether the processing takes place within the EU or not. [27]

[B] Entities Established Outside the EU

The GDPR may also apply to data controllers and data processors not established in the EU or EEA. This is the case when their processing activities are related to (1) the offering of goods or services to EU/EEA residents, whether or not the activity is connected to a payment, or (2) the monitoring of the behavior of EU residents when their behavior takes place within the EU. [28]

In November 2019, the European Data Protection Board (EDPB) published a final draft of its Guidelines 3/2018 on the Territorial Scope of GDPR Art. 3. [29] The document provides useful insights on the interpretation of GDPR Article 3.

[C] Main Establishment of Controller or Processor

If a data controller is established in more than one Member State, its main establishment is normally the place of its central administration located in the EU. However, if decisions on the purposes and means of processing of personal data are made in another establishment of the controller in the EU and if that other establishment has power to have such decisions implemented, the establishment making such decisions will be considered as the main establishment. [30]

If a data processor is established in more than one Member State, the main establishment is the place where the processor has its central administration in the EU. If the data processor has no central administration in the EU, the place where the main processing activities take place in the EU will be the main establishment. [31]

[D] EU Representative

GDPR Art. 4(17) defines a “representative” as a natural or legal person who represents the controller or processor with regard to their respective obligations under the GDPR. When a data controller or data processor is subject to GDPR Art. 3(2), it must designate in writing a representative in the EU, except if the processing is occasional and does not include, on a large scale, processing of special categories of data or data relating to criminal convictions and offenses and is unlikely to result in a risk to the rights and freedoms of individuals. [32]

The representative must be established in one of the Member States where the data subjects whose personal data are processed are located. Its primary role is to receive communications from the data protection supervisory authorities and data subjects on all issues related to the processing of personal data and to ensure compliance with the GDPR. [33]

Footnotes

27 GDPR Art. 3(1).

28 GDPR Art. 3(2).

29 Text of the Guidelines on territorial scope, *available at* https://edpb.europa.eu/ sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.

30 GDPR Art. 4(16)(a).

31 GDPR Art. 4(16)(b).

32 GDPR Art. 27.

33 GDPR Art. 27.

Global Privacy and Security Law - Gilbert, § GRC.06, Greece,NATIONAL DATA PROTECTION LAW—PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA

Francoise Gilbert, Global Privacy and Security Law § GRC.06 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

[A] General Principles

GDPR Art. 5(1) sets forth six principles governing the processing of personal data.

- **Lawfulness, Fairness, and Transparency:** Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- **Purpose Limitation:** Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data Minimization:** Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which the data are processed.
- **Accuracy:** Personal data must be accurate and where necessary kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate in regard to the purpose for which they are processed are erased or rectified without delay.
- **Storage Limitation:** Personal data must be kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed.
- **Integrity and Confidentiality:** Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

There is no additional provision in Greek law.

[B] Accountability

The six principles listed above are supplemented with a separate requirement for accountability. Under the accountability principle of GDPR Art. 5(2), the data controller is responsible for compliance with the six principles outlined above. The data controller is expected to be able to demonstrate compliance with those six principles.

There is no additional provision in Greek law.

[C] Lawfulness of Processing

Lawfulness of the processing is a key principle of the GDPR. GDPR Art. 6(1) establishes the conditions for lawful processing for personal data. Under GDPR Art. 6(2), Member States may introduce additional provisions.

Under GDPR Art. 6(1), the processing of personal data (other than special categories of data, which are subject to special rules) is lawful only in six circumstances.

- **Consent:** The data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes;
- **Contract:** Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
- **Legal Obligation:** Processing is necessary for compliance with a legal obligation to which the controller is subject;

- **Vital Interest:** Processing is necessary to protect the vital interests of the data subject or another individual;
- **Public Interest:** Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- **Legitimate Interest:** Processing is necessary to the purposes of the legitimate interests pursued by the controller or by a third party, except when such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection of personal data, in particular when the data subject is a child.

[D] Consent as Basis for Lawful Processing

GDPR Art. 6(1)(a) allows the processing of personal data when "the data subject has given consent to the processing or his or her personal data for one or more specific purposes." GDPR Art. 4(11) defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

GDPR Art. 7(1) defines the conditions for consent and states that, where processing is based on consent, a controller must be able to demonstrate that the data subject has consented to the processing of his or her data.

GDPR Art. 7(2) provides that the request for consent must be presented in a matter that is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. GDPR Art. 7(3) grants the data subjects the right to withdraw their consent at any time.

[E] Legitimate Interest as a Legal Basis for Processing

GDPR Art. 6(1)(f) allows the processing of personal data when it is necessary "for the purposes of the legitimate interest of the data controller or of a third party." However, this legitimate interest must be balanced against the interest or fundamental rights and freedoms of the individuals. Processing for the legitimate interest of the controller or a third party must not override the interests or the fundamental rights and freedoms of the data subjects that require protection of personal data. The analysis must take into account the data subjects' reasonable expectations based on their relationship with the controller and balance the interest of the controller. [34]

[F] Processing of Special Categories of Data

Different rules apply to the processing of "special categories of data." The term "special categories of data" includes personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; the processing of genetic data or biometric data in order to uniquely identify a natural person; and data concerning health or a person's sex life or sexual orientation.

[1] GDPR Provisions

The processing of data that meet the definition of special categories of data is prohibited, except in 10 cases listed in GDPR Art. 9(2). These exceptions include the following:

- **Explicit Consent:** The data subject has given explicit consent to the processing except where EU or Member State law provides that the prohibition may not be lifted by the data subject.
- **Employment, Social Protection:** The processing is necessary for carrying out the obligations and exercising specific rights of the controller or the data subject in the field of employment, social security, and social protection law as far as it is authorized by EU or Member State law or by a collective agreement.

- **Vital Interest:** The processing is necessary to protect the vital interests of the data subject or another individual when the data subject is physically or legally incapable of giving consent.
- **Non-Profit Body:** The processing is carried out in the course of legitimate activities by a foundation, association, or non-profit entity; relates solely to that entity's members or former members; and the data are not disclosed to others without the consent of the data subjects.
- **Data Already Made Public:** The processing relates to personal data that are manifestly made public by the data subject.
- **Exercise of Defense of Legal Claims:** The processing is necessary for the establishment, exercise, or defense of legal claims or whenever courts are acting in their judicial capacity.
- **Substantial Public Interest:** The processing is necessary for reasons of substantial public interest on the basis of EU or Member State law that must be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable measures to safeguard the fundamental rights and interests of the data subject.
- **Health, Diagnosis, Social Care:** The processing is necessary for preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, provision of health or social care or treatment or management of health or social care systems and services on the basis of EU or Member State law or pursuant to a contract with a health professional.
- **Public Health:** The processing is necessary for reasons of public interest in the area of public health, subject to appropriate protection and professional secrecy.
- **Archiving and Research:** The processing is necessary for archiving purposes in the public interest, scientific and historical research, or statistical purposes based on EU or Member State law, which must be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

[2] Greece-Specific Provisions

In Greece Law 4624/2019 [35] provides that, by derogation from GDPR Art. 9(1), processing of special categories of personal data by public and private bodies is permitted, if necessary, for purposes of:

- Exercising rights deriving from social security and social protection rights and for carrying out relevant obligations;
- Predictive medicine, evaluation of the employee's ability to work, medical diagnosis, provision of health or social care, administration of health or social care systems and services, or under contract with a health professional or other persons bound or supervised by professional secrecy; or
- Public interest in the public health sector, such as serious cross-border health threats, or to ensure high quality and safety standards for healthcare and medicinal products or medical devices.

The Hellenic Data Protection Authority has criticized the language used in Law 4624/2019 to regulate processing of special categories of personal data, [36] essentially arguing that it is poorly drafted, and it can create legal uncertainty. The relevant Greek provision seems to generally regulate all special categories of personal data, while, according to the “opening clause” of GDPR Art. 9(4), further conditions can be introduced by Member States specifically ***only*** with regard to the processing of genetic data, biometric data or data concerning health. The Authority has also pointed out that Law 4624/2019 is essentially a repetition of the relevant provisions of GDPR Art. 9(2), without, however, introducing any further conditions or limitations. Moreover, the Authority, comparing the exceptions listed in GDPR Art. 9(2) with the corresponding provision as included in Law 4624/2019, [37] has highlighted certain discrepancies, [38] which accentuates legal uncertainty regarding the interpretation of Law 4624/2019.

Further exceptions have been introduced by Law 4624/2019 [39] specifically for public bodies, which may process special categories of personal data, when

- Absolutely necessary for reasons of substantial public interest; [40]

- Necessary for the prevention of important threat to national security or public security; [41] or
- Necessary in order to take humanitarian measures, when the interest in processing overrides the interest of the data subject. [42]

The above exceptions apply under the condition that measures to safeguard data subjects' interests are taken. In addition, by derogation from GDPR Art. 9(1), Law 4624/2019 [43] provides that processing of genetic data for health and life insurance is expressly prohibited. [44]

Moreover, special categories of data may be processed in the context and for the purposes of an employment agreement, if necessary for the exercise of rights or the fulfilment of legal obligations arising from labor law, social security law, and social protection, when there is no reason to deem that processing is overridden by the legitimate interests of the data subject.

Under Law 4624/2019, [45] processing of special categories of data is also permitted when necessary to ensure freedom of expression and the right to information, including for journalistic, academic, artistic or literary purposes; such processing must be limited to the extent necessary and must take into account the data subject's right to personal and family right.

Further derogations from GDPR Art. 9(1) have been introduced by Law 4624/2019. Processing of special categories of personal data is permitted

- When necessary for archiving purposes in the public interest; [46] and
- Without the consent of the subject, when necessary for scientific or historical research purposes or statistical purposes, when the controller's interest overrides the data subject's interests. [47]

Both above derogations are subject to appropriate safeguard, which indicatively and most importantly include access restrictions, pseudonymization, encryption, and appointment of a Data Protection Officer (DPO). It should be noted that the personal data in question must be anonymized as soon as scientific or statistical purposes allow, unless this is in conflict with the legitimate interest of the data subject. Until then, the attributes, which can be used to match individual details regarding the personal or actual status of an identified or identifiable person, must be stored separately. Such attributes can be combined with the individual details, only if the research or statistical purpose so requires.

[G] Processing of Personal Data About Children

[1] GDPR Provisions

Under GDPR Art. 8, in relation to the offer of information society services directly to a child, a child's consent for the processing of their personal data is lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing is lawful only to the extent that consent is given by the holder of parental responsibility over the child and the controller has made reasonable efforts to verify, in such cases, that the consent is given by the holder of the parental responsibility over the child, taking into consideration available technology. [48]

Member States are permitted to change this age limit to between 13 and 16 years.

[2] Greece-Specific Provisions

Where personal data of data subjects below the age of 18 years are processed on the basis of consent, such consent, such processing is lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.

By way of exception, pursuant to GDPR Art. 8 in conjunction with Law 4624/2019, [49] in relation to the offer of information society services directly to a child, the age limit of lawful consent is reduced to 15 years. Where the child's age is below the age of 15, consent by the child's " *legal representative*" is required.

According to the relevant Explanatory Report, " *legal representative* " would be the person exercising parental care over the child (per Art. 1510 of Greek Civil Code) or a guardian (per Art. 1589 of Greek Civil Code). The controller bears the burden of proof that consent has been provided by a " *legal representative* ."

[H] Processing of Personal Data About Criminal Convictions and Offenses

[1] GDPR Provisions

GDPR Art. 10 focuses on the processing of personal data relating to criminal convictions and offenses. It provides that the processing of personal data relating to criminal convictions and offenses, as defined under GDPR Art. 6(1), may be carried out only under the control of official authority or when authorized by specific EU or Member State law. Further, any comprehensive register of criminal convictions may be kept only under the control of official authorities. [50]

[2] Greece-Specific Provisions

In addition, in Greece, under Law 4624/2019, [51] special categories of data and information about criminal prosecutions, convictions, and related security measures may be processed when necessary to ensure freedom of expression and the right to information, including for journalistic, academic, artistic or literary purposes; such processing must be limited to the necessary extent and also take into account the data subject's right to personal and family life.

Footnotes

34 GDPR Preamble § 47.

35 Law 4624/2019 Art. 22(1).

36 Hellenic Data Protection Authority, Opinion 1/2020, p. 11-14.

37 Law 4624/2019 Art. 22(1).

38 For instance, "occupational medicine" is not included in the Greek version of GDPR Art. 9(2)(h). Moreover, terminology used in the GDPR is changed in the Greek law: e.g., "ensuring high standards of quality" has changed to "ensuring high specifications of quality."

39 Law 4624/2019 Art. 22(2).

40 The Hellenic Data Protection Authority has questioned the legality of such exception (Opinion 1/2020, p. 12), arguing that this is not "clear and precise" (GDPR Preamble § 41): More specifically, while the said exception essentially repeats part of the exception provided by GDPR Art. 9(2)(g), it fails to introduce suitable and specific measures so that the substantial public interest is *"proportionate to the aim pursued, respect the essence of the right to data protection . "*

41 The Hellenic Data Protection Authority has questioned the legality of such exception (Opinion 1/2020, p. 13), arguing that such derogation is not based on a GDPR "opening clause."

42 The Hellenic Data Protection Authority has questioned the legality of such exception (Opinion 1/2020, p. 14), arguing that this is not based on an authorization provided by GDPR Art. 9.

43 Law 4624/2019 Art. 23.

44 The Hellenic Data Protection Authority has argued (Opinion 1/2020, p. 14) that such prohibition should also apply in the context of employment relationships.

45 Law 4624/2019 Art. 28(1)(d).

46 Law 4624/2019 Art. 29(1).

47 Law 4624/2019 Art. 30(1).

48 GDPR Art. 8(2).

49 Law 4624/2019 Art. 21.

50 While GDPR Art. 10 includes an "opening clause," which Member States can use in order to introduce national regulation regarding processing of such personal data providing for appropriate safeguards for the rights and freedoms of data subjects, Greek Law 4624/2019 has, notably, not done so.

51 Law 4624/2019 Art. 28(1)(d).

Global Privacy and Security Law - Gilbert, § GRC.07, NATIONAL DATA PROTECTION LAW—Data Subjects Rights

Francoise Gilbert, Global Privacy and Security Law § GRC.07 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

[A] Overview of the Data Subject Rights

[1] Overview

[a] *GDPR Provisions*

Data subjects are granted a wide variety of rights, including the following rights:

- Information
- Access
- Rectification
- Erasure
- Restriction of processing
- Portability
- Objection
- Not to be subject to automated decisions, including profiling

GDPR Art. 12(3) requires controllers to respond to a data subject's request without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, and the controller must inform the data subject of any such extension within one month of receipt of the request and provide the reasons for the delay. Where the data subject makes the request by electronic means, the information must be provided by electronic means where possible, unless the data subject requests otherwise.

[b] *Greece-Specific Provisions*

As explained below, Law 4624/2019 [52] has introduced extensive restrictions on the scope of the above-mentioned rights of data subjects, without, however, having introduced, as relevant, specific provisions as to the items mentioned in GDPR Art. 23(2) (e.g., processing purposes, categories of data, scope of restrictions, safeguards to prevent abuse or unlawful access or transfer, risks to the rights and freedoms of data subjects, etc.). In this context, the Hellenic Data Protection Authority has expressly [53] noted that, in the exercise of its powers, it will determine whether the relevant restrictions, as applied in each case, are in accordance with

the GDPR, the requirements set out in the Charter of Fundamental Rights of the European Union [54] and the European Convention for the Protection of Human Rights and Fundamental Freedoms. [55]

[B] Right to Information

[1] GDPR Provisions

Data subjects have the right to be informed about the processing of their personal data. This is a key transparency requirement under the GDPR. GDPR Arts. 13 and 14 set out the information to be provided to data subjects depending on whether the data were provided by the data subjects or not.

[a] *If the Data Subject Provided the Data*

When personal data relating to a data subject is collected from the data subject, GDPR Art. 13 requires that the controller provide the data subject with all of the following information when the information is obtained:

- The identity and the contact details of the controller and, where applicable, of the controller's representative;
- The contact details of the data protection officer, where applicable;
- The purposes of the processing for which the personal data are intended, and the legal basis for the processing;
- If the processing is conducted for the legitimate interests pursued by the controller or by a third party, a description of the legitimate interest;
- The recipients or categories of recipients of the personal data, if any;
- Whether the controller intends to transfer personal data to a third country reference to the appropriate or suitable safeguards and how to obtain a copy of the personal data or where they have been made available;
- The retention period, or if that is not possible, the criteria used to determine that period;
- The existence of the right to request from the controller access to, or rectification or erasure of personal data, or restriction of processing, right to object to processing, and right to data portability;
- Where the processing is based on consent, the existence of the right to withdraw consent at any time;
- The right to lodge a complaint with a supervisory authority;
- Whether the provision of personal data is a statutory or contractual requirement, or is necessary to enter into a contract, and whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data; and
- The existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, and the significance and envisaged consequences for the data subject.

[b] *If the Data Subject Did Not Provide the Data*

Where personal data have not been obtained from the data subject, GDPR Art. 14 requires the controller to provide the data subject with the following information within a reasonable period after obtaining the personal data, but at the latest within one month or, if the personal data is to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or if a disclosure to another recipient is foreseen, at the latest when the personal data are first disclosed. The information to be provided includes:

- The identity and the contact details of the controller and, where applicable, of the controller's representative;
- The contact details of the data protection officer, where applicable;

- The purposes of the processing for which the personal data are intended and the legal basis for the processing;
- The categories of personal data concerned;
- The recipients or categories of recipients of the personal data, if any;
- Where applicable, that the controller intends to transfer personal data to a third country and reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available;
- The retention period, or if that is not possible, the criteria used to determine that period;
- Whether the processing is conducted for the legitimate interests pursued by the controller or by a third party, a description of the legitimate interest;
- The existence of the right to request from the controller access to, or rectification or erasure of personal data, or restriction of processing, right to object to processing, and right to data portability;
- Where the processing is based on consent, the existence of the right to withdraw consent at any time;
- The right to lodge a complaint with a supervisory authority;
- From which source the personal data originate, and if applicable, whether it came from publicly accessible sources; and
- The existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, and the significance and envisaged consequences for the data subject.

[2] Greece-Specific Provisions

In Greece, exceptions from the obligation to inform have been introduced by Law 4624/2019, [56] for example, to address situations where personal data are collected from the data subject and the controller intends to further process the personal data for a purpose other than that for which the personal data were originally collected from the data subject. In such case, the controller is not required to inform data subject per GDPR Art. 13(3), when [57] such notice:

- Relates to a further processing of data in written form, for which (processing) the controller directly addresses the data subject, the data processing purpose is compatible with the original purpose, communication with the data subject is not in digital form and, under the circumstances, the data subject's interest to be informed (in particular with regard to the context in which data were collected) is not deemed to be high;
- Would jeopardize national or public security and the controller's interest in not providing the information outweighs the data subject's interest;
- Would interfere with the establishment, exercise or defense of the legal claims and the controller's interest in not providing the information outweighs the data subject's interest;
- Would jeopardize the confidential transfer of data to public bodies;
- In case of processing by public bodies, would jeopardize the right performance of the controller's tasks [58] and the controller's interest in not providing the information outweighs the data subject's interest.

Where personal data have not been obtained from the data subject, a further exception from obligation to inform data subjects in accordance with GDPR Arts 14(1), (2), and (4) has been introduced by Law 4624/2019; [59]

- In case of public bodies, when (i) such provision of information would jeopardize the right performance of controller's tasks; [60] or (ii) would jeopardize national or public safety;
- In case of private bodies, when (i) such provision of information would jeopardize the establishment, exercise or defense of legal claims or processing includes personal data from private contracts and aims at preventing damages from commitment of criminal offences, unless the interest of the data subject in being informed prevails; or (ii) a competent public body has informed the controller that publication of data would jeopardize national defense, national security, and national safety.

A further exception is added to the those mentioned in GDPR Art. 14(5), when notice to data subject would disclose information, which, due to its nature (in particular, due to overriding legal interest of a third party), must remain confidential. [61]

[C] Right of Access

[1] GDPR Provisions

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: [62]

- The purposes of the processing;
- The categories of personal data concerned;
- The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- The right to lodge a complaint with a supervisory authority;
- Where the personal data are not collected from the data subject, any available information as to their source;
- The existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and
- Information about the transfer of personal data to a third country, and the safeguards used for such transfer.

Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

[2] Greece-Specific Provisions

By derogation from GDPR Art. 15, in Greece, Law 4624/2019 [63] provides that a data subject's right of access may be restricted, when the exercise of such right is likely to render impossible or seriously impair the achievement of the objectives of archiving in the public interest and would involve a disproportionate effort.

Another derogation has been introduced by Law 4624/2019, [64] which provides that a data subject's right of access may be restricted, if necessary, when the exercise of such right is likely to render impossible or seriously impair the achievement of the objectives of processing for scientific or historical research purposes or for statistical purposes.

Furthermore, according to Law 4624/2019, [65] the exercise of the right of access is also restricted, when an exception from the obligation to inform data subject applies, where personal data have not been obtained from the data subject and (i) provision of information by a pubic body would jeopardize national or public safety; or (ii) in case of processing by a private body controller, a competent public body has informed the controller that publication of data would jeopardize national defense, national security, and national safety.

According to the same above provision, the exercise of the right of access is also restricted, when:

- Data have been recorded only because these cannot be deleted due to legal or regulatory data retention obligations; or

- Data are used exclusively for the protection or control of data, and the provision of access would involve a disproportionate effort, while the necessary technical and organizational measures make processing for other purposes impossible.

The reasons for the refusal to provide information must be documented and explained to the data subject, unless such explanation would jeopardize the purpose pursued via the refusal to provide the information.

A further exception to the GDPR Art. 15 right of access has been introduced, when the provision of access would disclose information, which, in accordance with a legal provision or due to its nature (in particular, due to overriding legal interest of a third party), must remain confidential. [66]

[D] Right to Rectification

[1] GDPR Provisions

The right to rectification means the right to obtain, without undue delay, the correction of personal data that are inaccurate or completion of personal data that are incomplete. [67]

[2] Greece-Specific Provisions

By derogation from GDPR Art. 16, in Greece, Law 4624/2019 [68] provides that a data subject shall not have a right to rectification, when the exercise of such right is likely to render impossible or seriously impair the achievement of the objectives of archiving in the public interest or the exercise of rights of third parties.

Moreover, by derogation from GDPR Art. 16, Law 4624/2019 [69] provides that a data subject's right to rectification may be restricted if necessary, when the exercise of such right is likely to render impossible or seriously impair the achievement of the objectives of processing for scientific or historical research purposes or for statistical purposes.

[E] Right to Erasure or “Right to be Forgotten”

[1] GDPR Provisions

The right of erasure means the right to obtain from the controller the erasure of personal data concerning the data subject without undue delay. [70] The data subject can request erasure where one of the following grounds applies:

- The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- The data subject withdraws consent on which the processing is based on consent and where there is no other legal ground for the processing;
- The data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purpose;
- The personal data have been unlawfully processed;
- The personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; or
- The personal data have been collected in relation to the offer of information society services in relation to the offer of information society services directly to a child based on their consent.

[2] Greece-Specific Provisions

In Greece, under Law 4624/2019, [71] the exercise of the right to erasure (GDPR Art. 17) is further restricted in cases of processing by means other than automated means, when, due to the special nature of data storage,

erasure is impossible or requires a disproportionate effort, and the interest of the data subject for erasure is not deemed important. In such cases the right to restriction of processing (GDPR Art. 18) would apply. Such restriction does not apply where the personal data have been unlawfully processed.

In addition, in case (i) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; or (ii) the personal data have been unlawfully processed, the exercise of the right to erasure is restricted to the extent the controller has reason to believe that the erasure would be prejudicial to the legitimate interests of the data subject.

In such a case, the right to restriction of processing [except from points (b) and (c) of GDPR Art. 18(1)] would apply. The controller must inform the data subject of the restriction of processing where such information is not impossible or does not involve a disproportionate effort.

Moreover, where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, the right to erasure is also restricted, if this is contrary to legal or contractual retention periods.

[F] Right to Restriction of Processing

[1] GDPR Provisions

GDPR Art. 18 grants data subjects the right to obtain from the controller restriction of processing of personal data in specific, limited circumstances. The data subject has the right to obtain from the controller restriction of processing where one of the following applies:

- The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims; or
- The data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject’s consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

[2] Greece-Specific Provisions

By derogation from GDPR Art. 18 (1)(a), (b), and (c), in Greece, Law 4624/2019 [72] provides that data subject's right to restriction may be limited, if necessary, when exercise of such right is likely to render impossible or seriously impair the achievement of the objectives of archiving in the public interest.

Another derogation is introduced by Law 4624/2019, [73] which provides that data subject's right to restrictions of processing may be limited, if necessary, when exercise of such right is likely to render impossible or seriously impair the achievement of the objectives of processing for scientific or historical research purposes or for statistical purposes.

[G] Right to Portability

[1] GDPR Provisions

The right to portability is the right to receive personal data concerning the data subject that the data subject previously provided to the controller. The data must be provided in a structured and commonly used machine-readable format, and the data subject may require that the data be transmitted to another controller without hindrance. [74]

The data subjects have the right to data portability only where the processing of personal data is based on their consent or on a contract to which the data subject is party and the processing is carried out by automated means.

[2] Greece-Specific Provisions

By derogation from GDPR Art. 20, in Greece, Law 4624/2019 [75] provides that a data subject's right to portability may be restricted, if necessary, when the exercise of such right is likely to render impossible or seriously impair the achievement of the objectives of archiving in the public interest.

[H] Right to Object

[1] GDPR Provisions

The right to object only applies in certain circumstances. Data subjects can object if the processing is for:

- A task carried out in the public interest;
- The exercise of official authority; or
- The legitimate interests pursued by the controller or by a third party.

In these circumstances, the right to object is not absolute. However, data subjects have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

[2] Greece-Specific Provisions

In Greece, an exception to the GDPR Art. 21 right to object has been introduced by Law 4624/2019, [76] according to which the right to object does not apply toward a public body, where:

- There is an imperative public interest for the processing, which overrides the data subject's interests; or
- A statutory provision makes the processing obligatory.

Moreover, by derogation from GDPR Art. 21, Law 4624/2019 [77] provides that data subject's right to object may be restricted, if necessary, when the exercise of such right is likely to render impossible or seriously impair the achievement of the objectives of archiving in the public interest.

Another derogation is introduced by Law 4624/2019, [78] which provides that a data subject's right to object may be restricted, if necessary, when the exercise of such right is likely to render impossible or seriously impair the achievement of the objectives of processing for scientific or historical research purposes or for statistical purposes.

[I] Right to Not Be Subject to Automated Decision Making, Including Profiling

The right to not be subject to a decision based solely on automated processing, including profiling, that produces legal effects concerning the data subject, including profiling is contained in GDPR Art. 22.

This right is not absolute; there are exceptions. Under GDPR Art. 22(2) the right does not apply if the decision is:

- Necessary for entering into, or the performance of, a contract between the data subject and the data controller;
- Authorized by Union or Member State Law to which the controller is subject, and that also lays down suitable measures to safeguard the data subject’s rights and freedoms; or

- Is based on the data subject's explicit consent.

There is no additional provision in Greek law.

Footnotes

52 Law 4624/2019 Arts. 31 to 35.

53 Hellenic Data Protection Authority Opinion 1/2020, p. 20.

54 Charter of Fundamental Rights of the European Union, Arts. 7, 8, and 52.

55 European Convention for the Protection of Human Rights and Fundamental Freedoms, Art. 8.

56 Law 4624/2019 Art. 31.

57 Apart from the case of GDPR Art. 13(4), i.e., where and insofar as the data subject already has the information.

58 In accordance with GDPR Art. 23(1)(a)–(e).

59 Law 4624/2019 Art. 32.

60 In accordance with GDPR Art. 23(1)(a)–(e).

61 Law 4624/2019 Art. 32(3).

62 GDPR Art. 15.

63 Law 4624/2019 Art. 29(2).

64 Law 4624/2019 Art. 30(2).

65 Law 4624/2019 Art. 33(1).

66 Law 4624/2019 Art. 33(4).

67 GDPR Art. 16.

68 Law 4624/2019 Art. 29(3).

69 Law 4624/2019 Art. 30(2).

70 GDPR Art. 17.

71 Law 4624/2019 Art. 34.

72 Law 4624/2019 Art. 29(4).

73 Law 4624/2019 Art. 30(2).

74 GDPR Art. 20.

75 Law 4624/2019 Art. 29(4).

76 Law 4624/2019 Art. 35.

77 Law 4624/2019 Art. 29(4).

78 Law 4624/2019 Art. 30(2).

Global Privacy and Security Law - Gilbert, § GRC.08, Greece,NATIONAL DATA PROTECTION LAW—CONTROLLERS' OBLIGATIONS *VIS-À-VIS* DATA SUBJECTS

Francoise Gilbert, Global Privacy and Security Law § GRC.08 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

[A] Transparency

Transparency is a key data protection principle. GDPR specifically addresses the principle of transparency by requiring that controllers provide data subjects with certain information about the processing of their personal data.

GDPR Art. 12 requires data controllers to take appropriate measures to provide any information referred to in GDPR Arts. 13 and 14, and any communication referred to in GDPR Arts. 15 to 22 and 34 in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

The information must be provided in writing, or by other means, including, where appropriate, by electronic means. In addition, it may be provided orally at the data subject's request, provided that the identity of the data subject is proven by other means.

[B] Other Obligations *Vis-à- Vis* Data Subjects

Data controllers have several obligations linked to the rights of a data subject in response to data subjects' requests. These include, for example, the obligation to facilitate the exercise of a data subject's rights (e.g., of information, access, erasure) (GDPR Arts. 15–17, 20) and to respond to data subjects' objections to the processing of their data or requests to restrict the processing (GDPR Arts. 18, 21).

There is no additional provision in Greek law.

Global Privacy and Security Law - Gilbert, § GRC.09, Greece,NATIONAL DATA PROTECTION LAW—OTHER OBLIGATIONS OF CONTROLLERS

Francoise Gilbert, Global Privacy and Security Law § GRC.09 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

The GDPR contains several provisions focusing on the operations of the data controller.

[A] Technical and Organization Measures to Ensure Compliance

GDPR Art. 24(1) requires data controllers to implement appropriate technical and organizational measures to ensure that the processing of personal data is performed in compliance with the GDPR. These measures must take into account the nature, scope, context, and purposes of the processing and the risks of varying likelihood and severity to the rights and freedoms of individuals. These measures must be reviewed and updated when necessary.

[B] Accountability

GDPR Art. 5(2) and 24(1) requires data controllers to demonstrate that their processing is performed in accordance with the GDPR.

[C] Recordkeeping Requirements for Data Controllers

GDPR Art. 30 requires data controllers to keep records of their processing activities. The records must be in writing, including in electronic form. The controller must be prepared to make these records available to the data protection supervisory authority on request.

The record of processing activities must contain the following information:

- The name and contact details of the data controller, and, where applicable, those of any joint controller, data controller's representative, and data protection officer;
- The purposes of the processing;
- The categories of data subjects;
- The categories of personal data;
- The categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries;
- If applicable, transfers of personal data to a third country (including the name of the country);
- If applicable, documentation that establishes the legal basis for any cross-border transfers and the related safeguards;
- When possible, the envisaged time limits for erasure of the different categories of data; and
- When possible, a general description of the technical and organizational security measures used to protect the personal data in the controller's custody.

Organizations with fewer than 250 employees are exempt from this recordkeeping requirement unless the processing:

- Is likely to result in a risk to the rights and freedoms of a data subject;
- Is not occasional;
- Includes special categories of data (e.g., health or trade union membership data); or
- Is conducted on data relating to criminal convictions and offenses.

[D] Data Protection by Design and by Default

[1] GDPR Provisions

GDPR Art. 25 requires data controllers to implement measures to ensure data protection by design and by default. These measures must take into account the state of the art, the cost of implementation, and the nature, scope, context, and purposes of processing, such as, for example, pseudonymization and data minimization. The measures must be adapted to face the varying risks to the rights and freedoms of natural persons posed by the processing.

[2] Dark Patterns as a Factor in Data Protection by Design and by Default

Data Protection by Design and by Default have been identified as essential factors in the EDPB’s analysis of dark patterns in social media platforms. The following elements are especially relevant to dark patterns:

- Autonomy—Data subjects should be granted the highest degree of autonomy possible to determine the use made of their personal data, as well as autonomy over the scope and conditions of that use or processing.
- Interaction—Data subjects must be able to communicate and exercise their rights in respect of the personal data processed by the controller.
- Expectation—Processing should correspond with data subjects’ reasonable expectations.
- Consumer choice—The controllers should not “lock in” their users in an unfair manner. Whenever a service processing personal data is proprietary, it may create a lock-in to the service, which may not be fair, if it impairs the data subjects’ possibility to exercise their right of data portability in accordance with Article 20 GDPR.
- Power balance—Power balance should be a key objective of the controller-data subject relationship. Power imbalances should be avoided. When this is not possible, they should be recognized and accounted for with suitable countermeasures.
- No deception—Data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design.

- Truthful—The controllers must make available information about how they process personal data, should act as they declare they will, and not mislead data subjects. [79]

[E] Data Protection Impact Assessment (DPIA)

[1] When a Data Protection Impact Assessment Is Required

[a] *GDPR Provisions*

When a proposed processing is likely to result in a high risk to the rights and freedoms of individuals, GDPR Art. 35 requires that the data controller assess the impact of the planned processing on the protection of personal data before commencing the processing.

GDPR Art. 35(3) identifies several situations where a DPIA is required:

- Systematic and extensive evaluation of personal aspects of natural persons that is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individuals or similarly significantly affect the individuals;
- Processing on a large scale of special categories of data or of data relating to criminal convictions and offenses is planned; or
- Systematic monitoring of a publicly accessible area on a large scale.

[b] *Greece-Specific Provisions*

On the basis of GDPR Art. 35(4), the Hellenic Data Protection Authority prepared a draft list of types of processing operations that are subject to the requirement for a DPIA. Before adopting the aforementioned DPIA list, the Greek Authority applied the consistency mechanism referred to in GDPR Art. 63 and communicated the draft DPIA list to the European Data Protection Board (EDPB). [80] At its plenary session of September 25, 2018, the EDPB issued its Opinion 7/2018 with recommendations on the Greek Authority's draft DPIA list, [81] on the basis of which, the Greek Authority further issued its Decision 65/2018, essentially amending the original DPIA; [82] the Greek Authority communicated the new list to the EDPB.

The Hellenic Data Protection Authority's DPIA list is based on, complements, and further specifies GDPR Art. 35 (in particular paragraphs 1 and 3 thereof) and also on the Article 29 Working Party Guidelines on DPIA. [83] As noted by the Greek Authority, the said list is not exhaustive; therefore, the obligations of the controller to carry out a DPIA in accordance with the requirement of GDPR Art. 35(1) and comply with all GDPR obligations remain unaffected.

[2] Content of the DPIA

GDPR Art. 35 defines the minimum content of a DPIA:

- Systematic description of the envisaged processing and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller;
- Assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- Assessment of the risks to the rights and freedoms of data subjects; and
- Measures planned to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned.

In addition, when appropriate, the data controller must seek the views of data subjects on the intended processing. [84]

[3] Prior Consultation with Supervisory Authority

[a] *GDPR Provisions*

When the DPIA indicates that the processing would result in a high risk for the data subjects in the absence of measures taken by the controller to mitigate the risk, GDPR Art. 36(2) requires the data controller to consult the supervisory authority before processing personal data unless the data controller elects to take specific measures to mitigate the risk.

If the supervisory authority determines that the intended processing would not comply with the GDPR, it must intervene within eight weeks following the request for consultation and give advice to the data controller. This period may be extended for a further six weeks, taking into account the complexity of the intended processing.

[b] *Greece-Specific Provisions*

The Hellenic Data Protection Authority (HDPA) has prepared a special form, which the controller must complete and submit electronically to request prior consultation with the Greek Authority. The controller can fill in the special form and submit it electronically [85] through the HDPA online portal; [86] alternatively and only if access to and use of the online portal is not possible for any documented reason, the controller can submit the prior consultation request by e-mail at *prior_consultation@dpa.gr*. [87] The form includes a section where the controller needs to confirm and establish that the request for prior consultation meets the typical requirements of GDPR Art. 36 and is, therefore, eligible for examination by the Greek Authority; it also includes a section where a description and documentation of the request must be added.

[F] Cooperation with the Supervisory Authority

GDPR Art. 31 requires a data controller and its representative, if any, to cooperate, on request, with the data protection supervisory authority in the performance of its tasks.

[G] Responsibilities of Joint Controllers

The GDPR contains numerous provisions defining the responsibilities and obligations for controllers regarding the processing and protection of personal data. This responsibility may be vested in several data controllers. Under GDPR Art. 26, if several data controllers jointly determine the purposes and means of processing personal data, they are deemed “joint controllers.”

In this case, the joint data controllers must determine their respective responsibilities for compliance with the obligations under the GDPR, in particular with respect to their respective duties to provide the information referred to the data subject with respect to the processing of the personal data, the allocations of their respective responsibilities to the data subject. The essence of the arrangement must be made available to the data subject, and the data subjects may exercise their GDPR rights against each of the controllers. [88]

Footnotes

79 EDPB Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognize and Avoid Them.

80 In accordance with GDPR Art. 35(6).

81 European Data Protection Board, Opinion 7/2018 on the draft list of the competent supervisory authority of Greece regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR), *available at* https:// edpb.europa.eu/our-work-tools/our-documents/valdybos-nuomone-64-str/opinion-72018-draft-list-competent-supervisory_en.

82 Decision 65/2018 has been officially published in Government Gazette (Series II, No 1622/10.05.2019).

83 Article 29 Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679" (WP 248 rev.01), adopted on 4 April 2017, as last revised and adopted on 4 October 2017), *available at* https://ec.europa.eu/newsroom/document.cfm?doc_id=47711.

84 GDPR Art. 35(9).

85 Only in exceptional cases the form can be submitted differently (e.g., in person), and in this case, the reason for not using electronic submission should be adequately documented

86 Prior registration with the online portal is needed.

87 The prior consultation request form is *available at* https://www.dpa.gr/sites/default/files/2020-11/PREVIOUS%20CONSULTATION%20REQUEST%20FORM.DOCX.

88 GDPR Art. 26(3).

Global Privacy and Security Law - Gilbert, § GRC.10, Greece,NATIONAL DATA PROTECTION LAW—DATA PROCESSORS

Francoise Gilbert, Global Privacy and Security Law § GRC.10 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

[A] Recordkeeping Requirements

Data processors have recordkeeping obligations that are very similar to those of the data controllers. Under GDPR Art. 30(2), the record must contain the following information:

- The name and contact details of the data processor or subprocessors; of each data controller on behalf of which the data processor is acting; and, when applicable, of the data controller's or data processor's representative and the data protection officer, if any;
- The categories of processing carried out on behalf of each data controller;
- If applicable, a description of the transfers of data to a third country and, in some instances, the documentation of appropriate safeguards; and
- When possible, a description of the technical and organizational security measures being used.

GDPR Art. 30(5) exempts organizations with fewer than 250 employees from this recordkeeping requirement unless the data processing (1) is likely to result in a risk to the rights and freedoms of a data subject, (2) is not occasional, (3) includes special categories of data (e.g., health or trade union membership data), or (4) is conducted on data relating to criminal convictions and offenses.

[B] Conditions for Processing Data by a Data Processor or Subprocessor

There are several significant conditions to the engagement of a data processor or subprocessor to process data on behalf of a data controller.

[1] Sufficient Guarantees

First, if a data controller intends to entrust a third party with the processing of personal data, GDPR Art. 28 requires the controller to engage only data processors that provide sufficient guarantees to implement appropriate technical and organizational measures to ensure that the processing can meet the GDPR requirements and ensure the protection of data subjects' rights.

[2] Written Data Processing Agreement Required

Second, GDPR Art. 28 requires that, when an entity engages a third party to process personal on its behalf, the terms of the engagement be governed by a contract or other legal act that binds the data processor to the data controller. The contract must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the data controller. It must require the data processor to:

- Process the personal data only on documented instructions from the data controller, including with regard to transfers of personal data to a third country, unless otherwise required by applicable law to which the data processor is subject;
- Ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Take all appropriate security measures required by GDPR;
- Enlist another data processor only with the prior specific or general written authorization of the data controller and pursuant to a written contract with at least the same data protection obligations as set out in the contract between the controller and the processor;
- Assist the data controller by appropriate technical and organizational measures that take into account the nature of the processing in the fulfillment of the data controller's obligation to respond to data subjects' requests;
- Assist the data controller in ensuring compliance with its security obligations;
- At the data controller's choice, delete or return all the personal data to it after the end of the services relating to the processing, and delete existing copies unless EU or Member State law requires storage of the data; [89]
- Make available to the data controller all information necessary to demonstrate compliance with its obligations under GDPR, and allow for and contribute to audits and inspections conducted by the data controller or another auditor mandated by the data controller; and
- Immediately inform the data controller if, in his or her opinion, an instruction by the data controller breaches any provision of GDPR or any EU or Member State data protection provisions.

GDPR Art. 28(6) allows the contract between a data controller and a data processor to be based, in whole or in part, on standard contractual clauses.

In addition to the Art. 28 obligations, the data processing agreement must address the provisions of GDPR Articles 44 to 50, which provide the rules regarding the transfer of data across borders and outside the EU/EEA region.

[3] Controller’s Prior Authorization to the Use of Subprocessors

Third, GDPR Art. 28(2) prohibits a data processor from engaging another data processor without the prior written specific or general authorization of the controller. In the case of general written authorization, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

The contract with the subprocessor must include the same data protection obligations as those that are required in a contract between the data controller and the data processor. If the subprocessor fails to fulfill its data protection obligations, the primary data processor remains fully liable to the data controller for the performance of that subprocessor's obligations.

[4] No Further Processing Permitted

GDPR Art. 29 prohibits entities that are acting in a data processor and subprocessor capacity from processing personal data other than on instructions from the data controller, or from the applicable primary processor,

unless required to do so by applicable law. The prohibition applies directly to the data processor in addition to the terms of the required contract. This clause makes the data processor directly liable under the GDPR, and its failure to comply would be directly enforceable by the applicable data protection authority.

[5] Standard Contractual Clauses

As discussed above, when a controller engages a processor to provide data processing services, GDPR Art. 28 requires these entities to enter into a written agreement that meets the criteria specified in GDPR Art. 28 (1)-(5). In addition, GDPR Art 28(6) provides that entities planning to develop the terms of such written agreement may rely, in whole or in part, on standard contractual clauses. GDPR Art. 28 (7) and (8) grant the European Commission and the member state Data Supervisory Authorities the right to draft and adopt standard contractual clauses that meet the requirements of GDPR Art. 28.

In the context of the implementation of the GDPR, in June 2021, the European Commission published the final versions of two documents containing sample "Standard Contractual Clauses":

- One document provides a template that meets the requirements set forth in GDPR Art. 28 (processing conducted by a processor); [90]
- The other document provides four templates that meet the requirements set forth in GDPR Art. 46 (crossborder transfers when a party is located outside the EU/EEA). [91]

Out of these two documents, only the first one is relevant to this section. The second document is relevant the section that concerns crossborder data transfers and GDPR Art. 46, reviewed below in this chapter.

The first set of Standard Contractual Clauses listed above is intended to address the requirements of GDPR Art. 28, specifically those provisions concerning the content of data processing services agreement between a controller and a processor. [92] It is to be used ***only when the controller and the processor are both located in the EU/EEA***.

The second document listed above, which provides four templates (called modules), addresses the requirements of GDPR Art. 46(2) when personal data are transferred across borders outside the EU/EEA Region. That set of four templates is discussed below in this chapter in the section on GDPR Art. 46 and crossborder data transfers. [93] These templates were adopted by the European Commission under the authority granted by GDPR Art. 46 (2)(c). These templates are frequently designated as "Modernized Standard Contractual Clauses (SCC)" because they replace and supersede similar documents created in the period 2001 to 2010 while Directive 95/46/EC was in effect, in the context of Art. 26 of the now-repealed Directive 95/46/EC.

Footnotes

89 A data processor cannot keep the data in any case, unless otherwise provided by law. The data controller may choose whether the data processor will just delete the data or also return the personal data before deleting them from its own systems.

90 This document was drafted and adopted by the EU Commission pursuant to GDPR Art. 28(7).

91 This document was drafted and adopted by the EU Commission pursuant to GDPR Art. 46(2)(c).

92 These GDPR Art. 28 Standard Contractual Clauses are available at: https://ec. europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors.

93 These Standard Contractual Clauses for International Transfers are available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

Global Privacy and Security Law - Gilbert, § GRC.11, Greece,NATIONAL DATA PROTECTION LAW—DATA PROTECTION OFFICER

Francoise Gilbert, Global Privacy and Security Law § GRC.11 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

[A] Entities Required to Appoint Data Protection Officer

GDPR Art. 37 requires data controllers and data processors other than public authorities to designate a data protection officer (DPO) when the core processing activities of the controller or the processor consist of:

- Activities whose scope or purposes require regular and systematic monitoring of data subjects on a large scale, or
- Processing on a large-scale data that are part of the “special categories of data” (e.g., data pertaining to health or race) or data relating to criminal convictions and offenses.

In case the processing is carried out by a public authority or body, the appointment of a DPO is mandatory.

The controller or processor that has appointed a DPO must publish the DPO's contact details and communicate these details to the supervisory authority. [94]

A group of entities (e.g., the different companies in a corporate group) may appoint a single data protection officer, provided that the DPO is easily accessible from each establishment.

[B] Qualifications of a Data Protection Officer

GDPR Art. 37 identifies the basic requirements for engaging a DPO. The person should be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices, and the ability to fulfill the tasks normally assigned to a DPO. The DPO may be a staff member of the data controller or data processor. The function of the DPO may be outsourced to a third party on the basis of a contract for services.

[C] Position of Data Protection Officer

GDPR Art. 38 describes the framework for the position of DPO.

The DPO must report directly to highest management levels of the controller or processor, and the DPO must not receive instructions regarding the exercise of his/her task. The DPO may not be dismissed for performing his/her tasks. [95]

The data controller or processor must ensure that its DPO is involved in all issues that relate to the protection of personal data. It must provide the DPO with resources necessary to carry out the DPO's tasks, access to personal data and processing operations, and the means to maintain their expert knowledge.

[D] Tasks of Data Protection Officer

[1] GDPR Provisions

GDPR Art. 39 specifies the responsibilities of data protection officers. They include, for example:

- Inform and advise the entity and the employees who carry out processing of their obligations under GDPR;

- Monitor compliance with the GDPR and the applicable laws and with the policies of the controller or processor regarding personal data protection;
- Advise, when requested, on the conduct of a data protection impact assessment and monitor the performance of the assessment;
- Cooperate with the applicable supervisory authority; and
- Act as contact point for the applicable supervisory authority on issues related to the processing of personal data, including prior consultation.

[2] Greece-Specific Provisions

In Greece, Law 4624/2019 [96] repeats the obligation for all public bodies to appoint a DPO; there are also provisions in place regarding its role and duties, including an exception from the general rule [97] to publish the contact details of the DPO and communicate them to the supervisory authority, when this is required for reasons of national security or due to a duty of confidentiality provided by law. [98] The Hellenic Data Protection Authority has questioned the legality of such exception, arguing that this is not based on an "opening clause" or any other clause included in the GDPR. [99]

[E] Committee of Data Protection Officers of the Greek Central Government Bodies

By virtue of Article 26 of Greek Law 4961/2022, a Committee of Data Protection Officers is established, poised to coordinate actions and adopt best practices in the performance of the tasks of the data protection officers of the central government bodies. The Committee is established by joint decision of the Ministers of Justice and Digital Governance and meets, at the invitation of its chairman, regularly once a quarter and exceptionally when the chairman deems it necessary.

The Committee shall be composed of nine members and shall consist of DPOs appointed by the central government bodies referred to in point (c) of paragraph 1 of Article 14 of Law 4270/2014. Criteria for their selection include *inter alia* the type of personal data, the scale of processing, and the impact on the rights and freedoms of natural persons.

Footnotes

94 GDPR Art. 37(7).

95 GDPR Art. 38(3).

96 Law 4624/2019 Art. 6.

97 GDPR Art. 37(7).

98 Law 4624/2019 Art. 6(5).

99 Hellenic Data Protection Authority, Opinion 1/2020, p. 9-10.

Global Privacy and Security Law - Gilbert, § GRC.12, Greece,NATIONAL DATA PROTECTION LAW—SECURITY OF PERSONAL DATA; DATA BREACH

Francoise Gilbert, Global Privacy and Security Law § GRC.12 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

[A] Technical and Organizational Measures Required

Both controllers and processors are required to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of data processing. The measures must take into account the nature, scope, context, and purposes of the processing, the risk of varying likelihood and severity to the rights and freedoms of individuals, the state of the art, and the costs of implementation. [100] According to GDPR Art. 32, these measures must include, as appropriate:

- Pseudonymization;
- Encryption;
- Ensuring the ongoing confidentiality, integrity, availability, and resilience of systems and services processing personal data;
- Ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident; and
- Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

[B] Breach of Security

GDPR Art. 4(12) defines “personal data breach” as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.” [101]

[1] Notification of the Supervisory Authority

If there is a personal data breach, the data controller must, without undue delay, and when feasible not later than 72 hours after having become aware of it, give notice of the breach to the competent supervisory authority, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. [102] If notification is not made within 72 hours, the data controller must provide to the supervisory authority a reasonable justification explaining the reason for the delay.

The notification to the supervisory authority must provide at least the following information:

- Description of the nature of the breach, including when possible, the categories and approximate numbers of data subjects and data records concerned;
- Name and contact details of the data protection officer or other contact point where more information can be obtained;
- Description of the likely consequences of the personal data breach; and
- Description of the measures taken or proposed to be taken by the data controller to address the breach, including, when appropriate, to mitigate its possible adverse effects.

If it is not possible to provide all required information at the same time, this information may be provided in phases, without undue further delay.

The data controller must document a personal data breach, including the facts surrounding the breach, its effects, and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with the controller's obligation under the applicable provisions of the GDPR.

[2] Notification of the Data Subjects

[a] *GDPR Provisions*

GDPR Art. 34(1) requires the data controller that has suffered a personal data breach to notify the data subjects "without undue delay" when the personal data breach is likely to "result in a high risk to the rights and freedoms of individuals affected."

The communication to the data subject must describe in clear and plain language the nature of the personal data breach and contain at least the same information as that which has been provided to the Supervisory authority:

- Description of the nature of the breach, including when possible, the categories and approximate numbers of data subjects and data records concerned;
- Name and contact details of the data protection officer or other contact point where more information can be obtained;
- Description of the likely consequences of the personal data breach; and
- Description of the measures taken or proposed to be taken by the data controller to address the breach, including, when appropriate, to mitigate its possible adverse effects.

The communication to the data subject is not required if any of the following conditions are met:

- The controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;
- The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred above is no longer likely to materialize; and
- It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

In addition, if the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to above are met.

[b] *Greece-Specific Provisions*

The Hellenic Data Protection Authority, the competent supervisory authority, has published a breach notification form (along with instructions for filing), which the controller must use in order to electronically notify an incident to the Greek Authority; the controller can fill in and submit the form electronically through the Hellenic Data Protection Authority online portal; [103] controller which are not based in Greece (and, thus, are not able to register with the online portal) can submit the notification via email (at *databreach@dpa.gr*). [104] Only when the incident is with regard to "cross-border processing" (as defined by the GDPR) can notification be in English; otherwise notification must be filed in Greek. The Greek Authority also refers to the "Guidelines on Personal data breach notification under the GDPR" issued by the Article 29 Working Party. [105]

In case of a personal data breach, an exception to the obligation to notify data subjects in accordance with GDPR Art. 34 [106] has been introduced by Law 4624/2019, [107] when such notice would disclose information which, in accordance with a legal provision or due to its nature (in particular, due to overriding legal interest of a third party), must remain confidential. By way of derogation, the data subject shall be informed, [108] when his/her interests (in particular, taking into account the threat of damage) outweigh the interests of confidentiality.

Greece has, by virtue of Law 4727/2020, transposed Directive (EU) 2018/1972 establishing the European Electronic Communications Code (EECC). According to Article 148 of Law 4727/2020 (transposing Article 40 of EECC on security of networks and services), providers of public electronic communications networks or of publicly available electronic communications services must comply with certain security-related provisions and notification requirements, e.g., take appropriate and proportionate technical and organizational measures to appropriately manage the risks posed to the security of networks and services and notify, without undue delay, the Hellenic Authority for Communication Security and Privacy (ADAE) of a security incident that has had a

significant impact on the operation of networks or services (in the case of a particular and significant threat of a security incident, potentially affected users must also be informed).

[3] Breach Affecting a Data Processor

If the breach affects a data processor, it must notify the data controller without undue delay after becoming aware of a personal data breach. [109]

Footnotes

100 GDPR Art. 32.

101 Relevant are the EDPB Guidelines 1/2021 on Examples regarding Data Breach Notification, aiming to help data controllers in deciding how to handle data breaches and what factors to consider during risk assessment, *available at* https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_ en.pdf.

102 GDPR Art. 33.

103 Prior registration with the online portal is needed, using the tax credentials available to controllers established in Greece.

104 The breach notification form and instructions for filing are *available at* https:// www.dpa.gr/en/Organisations/Data_Breach_notification/Submission.

105 Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679 (WP250rev.01), adopted on 3 October 2017, as last revised and adopted on 6 February 2018, *available at* https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827.

106 Other than the exception provided by GDPR Art. 34(3).

107 Law 4624/2019 Art. 33(5).

108 In accordance with GDPR Art. 34.

109 GDPR Art. 33(2).

Global Privacy and Security Law - Gilbert, § GRC.13, Greece,NATIONAL DATA PROTECTION LAW—CROSSBORDER DATA TRANSFERS

Francoise Gilbert, Global Privacy and Security Law § GRC.13 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

GDPR Arts. 44–49 define the rules applicable to crossborder data transfers. Any transfer of personal data to a third country for processing may take place only if the data controller and data processor comply with rules regarding the transfer of personal data to third countries as set forth in GDPR Arts. 44–49.

[A] Transfers on the Basis of an Adequacy Decision

Transfer of personal data to a third country may take place when the EU Commission has determined that the receiving country ensures an adequate level of protection. [110]

Since the GDPR does not provide for a legal definition of the notion “transfer of personal data to a third country or to an international organization,” the EDPB identified three cumulative criteria that qualify a processing as a transfer:

- A controller or a processor is subject to the GDPR for the given processing.
- This controller or processor (“exporter”) discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller, or processor (“importer”).
- The importer is in a third country or is an international organisation, irrespective of whether this importer is subject to the GDPR in respect of the given processing in accordance with Art. 3 of the GDPR. [111]

GDPR Arts. 45(4) and 45(9) allow for the survival of the adequacy decisions adopted by the EU Commission on the basis of Article 25(6) of Directive 95/46/EC until these decisions are amended, replaced, or repealed by a Commission decision.

Currently, the countries outside the European Economic Area (EEA) that have been recognized as providing adequate protection include Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom (under the GDPR and the Law Enforcement Directive) and Uruguay. [112]

With the exception of the United Kingdom, these adequacy decisions do not cover data exchanges in the enforcement sector, which are governed by Art. 36 of the EU Law Enforcement Directive. [113]

Transfers to a third country that does not meet the conditions above are not possible unless an exception or a derogation applies. GDPR Articles 45, 46, and 49 provide the rules that apply when the data is to be transferred and/or processed in a country for which the EU Commission has not made a determination that the country offers adequate protection.

[B] Transfers by Way of Appropriate Safeguards

[1] General Rules

In the absence of an adequacy decision as discussed above, a data controller or data processor may transfer personal data to a third country only if the data controller or data processor has provided appropriate safeguards and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available. [114]

The “appropriate safeguards” set forth in GDPR Art. 46(1) may be provided, without a specific authorization from a supervisory authority, by:

- A legally binding and enforceable instrument between public authorities or bodies;
- Binding Corporate Rules;
- Standard data protection clauses adopted by the EU Commission;
- Standard data protection clauses adopted by a supervisory authority and approved by the EU Commission;
- An approved code of conduct with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including those that pertain to data subjects' rights; or
- An approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including those regarding data subjects' rights.

[2] Binding Corporate Rules

GDPR Art. 47 establishes the legitimacy of the Binding Corporate Rules (BCR) as a means to show adequacy in relations to crossborder data transfer. GDPR Art. 47 also establishes the rule regarding the content and approval of BCR.

To be eligible for approval by the competent data supervisory authority, proposed BCR must meet two sets of criteria. First, under GDPR Art. 47(1), they must:

- Be legally binding and apply to and are enforced by every member of a group of entities or groups of enterprises engaged in a joint economic activity, including their employees;
- Expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and
- Fulfill the requirements set forth in GDPR Art. 47(2).

Second, the BCR must contain the content specified in GDPR Art. 47(2). To meet this obligation, BCR shall specify at least:

- The structure and contact details of the group of enterprises engaged in a joint economic activity and of each of its members;
- The data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
- Their legally binding nature, both internally and externally;
- The application of the general data protection principles, in particular purpose limitation, data minimization, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements for onward transfers to bodies not bound by the binding corporate rules;
- The rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;
- The acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union;
- How the information on the binding corporate rules is provided to the data subjects;
- The tasks of any data protection officer or any other person or entity in charge of the monitoring compliance with the BCR within the group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;
- The complaint procedures;
- The mechanisms within the group of enterprises for ensuring the verification of compliance with the BCR, including data protection audits and methods for ensuring corrective actions to protect the rights of the data subject;
- The mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;
- The mechanisms for cooperation with the supervisory authority to ensure compliance by any member of the group of enterprises, in particular by making available to the supervisory authority the results of verifications of the measures;
- The mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group enterprises is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the BCR; and
- The appropriate data protection training to personnel having permanent or regular access to personal data.

[3] Standard Contractual Clauses

GDPR Art. 46(2) also allows businesses intending to receive data from an EU or EEA Member State to enter into a contract with the data exporter in which the two entities commit to provide adequate safeguards for the data.

[4] The Demise of the EU-U.S. Privacy Shield and Its Aftermath

[a] *The Court of Justice of the EU (CJEU) Schrems II Ruling*

In July 2020, the Court of Justice of the EU (CJEU) delivered its landmark judgment in Case C-311/18 *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* (*Schrems II*), [115] essentially declaring the EU-US Privacy Shield invalid and, most importantly, questioning the extent to which EU-based organizations can still rely on the European Commission's Standard Contractual Clauses (SCCs) for data processing outsourced to providers in the United States and globally.

The CJEU found that, before a transfer of data may occur, there must be a prior assessment of the context of each individual transfer, that evaluates the laws of the country where the recipient is based, the nature of the data to be transferred, the privacy risks to such data, and any additional safeguards adopted by the parties to ensure that the data will receive adequate protection, as defined under EU Law. Further, the data importer is required to inform the data exporter of any inability to comply with the standard data protection clauses. If such protection is lacking the parties are obligated to suspend the transfer or terminate the contract.

While the concept of using SCCs—especially those issued by the EU Commission—remains valid, the continued validity is subject to an additional step: the obligation to conduct the equivalent of a data protection impact assessment to ensure that the adequate protection is and will be provided and subsequently, continuously monitored.

The Hellenic Data Protection Authority has published a summary of *Schrems II* , also referring to the FAQ on *Schrems II* adopted and published by the EDPB on July 23, 2020. [116] The Hellenic Data Protection Authority points out that as a follow-up to the *Schrems II* ruling, the EDPB has created a taskforce that will prepare recommendations to assist controllers and processors with their duty to identify and implement appropriate supplementary measures to ensure adequate protection when transferring data to third countries.

[b] *The Aftermath of the* Schrems II *Ruling*

The EDPB published for comments several important recommendations and guidelines:

- Recommendations 01/2020 on measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, adopted on November 10, 2020 and finalized in June 2021; [117] and
- Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures, adopted on November 10, 2020. [118]

In these Recommendations, the EDPB outlined suggested acceptable measures to implement the guidance outlined in the *Schrems II* decision, which required among other things the conduct of an investigation similar to a data protection impact assessment, where the data exporter would evaluate, in the context of each individual transfer, the laws of the country where the recipient is based, the nature of the data to be transferred, the privacy risks to such data, and any additional safeguards adopted by the parties to ensure that the data will receive adequate protection, as defined under EU Law.

[c] *The Draft Adequacy Decision for the EU-U.S. Data Privacy Framework*

In December 2022, the European Commission launched the process to adopt an adequacy decision [119] for the EU-U.S. Data Privacy Framework, which will foster Trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union in its *Schrems II* ruling. The adoption process involves obtaining an opinion from the European Data Protection Board and the green light from a committee composed of representatives of EU Member States. In addition, the European Parliament has a right of scrutiny over adequacy decisions.

The proposal for a draft adequacy decision follows the adoption of an Executive Order on "Enhancing Safeguards for United States Signals Intelligence Activities" by U.S. President Biden in October 2022. Along with

the Regulation issued by the Attorney General, the Executive Order implements into U.S. law the agreement in principle on a new EU-U.S. Data Privacy Framework that was announced in March 2022 by President von der Leyen and President Biden, following more than one year of negotiations.

[5] The Modernized Standard Contractual Clauses (June 2021)

On June 4, 2021, the European Commission issued updated versions of the standard contractual clauses for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR), which replace the three precious sets of SCCs that were adopted under Directive 95/46. [120] The new SCCs combine general clauses with a modular approach to cater for various transfer scenarios and the complexity of modern processing chains. In addition to the general clauses, controllers and processors should select the module applicable to their situation, so as to tailor their obligations under the standard contractual clauses to their role and responsibilities in relation to the data processing in question.

The current version of the form agreement to be used is found in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. [121]

- Module One: Transfer Controller to Controller
- Module Two: Transfer Controller to Processor
- Module Three: Transfer Processor to Processor
- Module Four: Transfer Processor to Controller

[C] Derogations for Specific Situations

In the absence of an adequacy decision or appropriate safeguards, such as BCRs or Standard Contractual Clauses, GDPR Art. 49 allows transfers of personal data in a number of specific circumstances. These circumstances include:

- The data subject has explicitly consented to the proposed transfer after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken at the data subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- The transfer is necessary for important reasons of public interest;
- The transfer is necessary for the establishment, exercise, or defense of legal claims;
- The transfer is necessary to protect the vital interests of the data subject or other persons when the data subject is physically or legally incapable of giving consent; or
- The transfer is made from a register that, under EU or Member State law, is intended to provide information to the public and that is open to consultation by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by the EU or Member State law for consultation are fulfilled in the particular case.

In those circumstances, the transfer may occur only if:

- It is not repetitive, concerns only a limited number of data subjects, and is necessary for the purposes of compelling legitimate interests pursued by the data controller that are not overridden by the interests or rights and freedoms of the data subject; and
- The controller has assessed all the circumstances surrounding the data transfer and based on this assessment, it adduced suitable safeguards with respect to the protection of personal data.

The data controller must inform the competent supervisory authority and the concerned data subjects about the proposed transfer and the compelling legitimate interests pursued by the data controller.

[D] Transfers or Disclosures in the Context of Litigation

Special rules apply to transfer of data in connection with litigation. Under GDPR Art. 48, any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a data controller or data processor to transfer or disclose personal data may only be recognized or enforceable if it is based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the EU or a Member State, without prejudice to other grounds for transfer.

In addition, a number of Member States have adopted "blocking statutes" that prohibit certain transfers of data —personal or not—in connection with litigation. These blocking statutes were enacted to protect valuable commercial information from being transferred abroad, out of a concern that the U.S. rules of procedure might give U.S. litigants the opportunity to have access to valuable confidential information under the guise of discovery requests.

There is no additional provision in Greek law.

Footnotes

110 GDPR Art. 45(1).

111 EDPB Guidelines 05/2021 on the Interplay Between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR.

112 Current list, *available at* https://ec.europa.eu/info/law/law-topic/data-protection/ international-dimension-data-protection/adequacy-decisions_en.

113 Directive (EU) 2016/680.

114 GDPR Art. 46(1).

115 http://curia.europa.eu/juris/liste.jsf?num=C-311/18.

116 https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf.

117 EDPB Recommendations 01/2020 Version 2.0, *available at* https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

118 Recommendations 02/2020, *available at* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf.

119 The draft adequacy decision is available at https://commission.europa.eu/system/ files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf.

120 Commission Implementing Decision (EU) 2021/914, *available at* https://eur-lex. europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en.

121 These new Standard Contractual Clauses for International Transfers are *available at* https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data- protection/standard-contractual-clauses-scc_en.

Global Privacy and Security Law - Gilbert, § GRC.14, Greece,NATIONAL DATA PROTECTION LAW—CODES OF CONDUCT AND CERTIFICATION MECHANISMS

Francoise Gilbert, Global Privacy and Security Law § GRC.14 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

GDPR Arts. 40 to 43 allow for the creation of codes of conducts and certification bodies intended to help entities subject to the GDPR demonstrate their compliance with the law. Codes of conduct will provide a structure that entities subject to the Regulation could follow in order to self-certify their adherence to that code of conduct. Certification bodies would attest of the compliance by auditing applicants and verifying that the applicant practices conform to the required rules. Numerous sections of the GDPR make reference to compliance with a Code of Conduct or a certificate from a certification body as a means to demonstrate compliance with relevant provisions of the GDPR.

[A] Codes of Conduct

[1] GDPR Provisions

GDPR Art. 40 prompts Member States, supervisory authorities, as well as the EDPB and EU Commission to encourage the creation of codes of conduct to assist in the proper implementation of the GDPR in specific sectors, or by specific categories of businesses, such as micro, small, and medium-sized enterprises.

The codes of conduct are to be prepared by associations and other bodies representing categories of controllers or processors, and are to address specific aspects of the GDPR, such as those concerning fair and transparent processing; legitimate interest; collection of personal data; pseudonymization of personal data; information provided to the public and to data subjects; the exercise of the rights of data subjects; the handling of children personal information; measures and procedures that controllers and processors must take to show their compliance with the GDPR, security obligations; data breach notification obligations; cross border data transfers or the handling of disputes.

Codes of conduct may be specific to a Member State or may relate to processing activities in several Member States. After review by the relevant supervisory authority or authorities, the EU Commission may decide that the approved code of conduct has general validity within the entire Union.

Without prejudice to the tasks and powers of the competent supervisory authority, the monitoring of compliance with a code of conduct pursuant to GDPR Art. 40 may be carried out by a body that has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority. [122] Moreover, a code of conduct shall contain mechanisms which enable the said body to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent. [123]

The EDPB has published its “Guidelines 04/2021 on codes of conduct as tools for transfers,” providing practical guidance on this issue, including on the content of such codes of conduct, their adoption process and the actors involved, as well as the requirements to be met and guarantees to be provided by a code of conduct for transfers. [124]

[2] Greece-Specific Provisions

The Hellenic Data Protection Authority has decided on requirements for accreditation of monitoring bodies; [125] the said requirements are based on the EDPB “Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679” and have been submitted to the EDPB, pursuant to the consistency mechanism referred to in GDPR Art. 63; the EDPB has published Opinion 20/2020 on the draft decision of the competent supervisory authority of Greece regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Article 41 of GDPR. [126]

[B] Certification

[1] GDPR Provisions

Member States, supervisory authorities, the EDPB, and the EU Commission may also, as provided in GDPR Art. 43, encourage the establishment of data protection certification mechanisms and data protection seals and marks, through which controllers and processors can demonstrate their compliance with the Regulation. The certification will be issued by certification bodies that have been accredited by the competent supervisory authority or a national accreditation body named in accordance with Regulation (EC) No. 765/2008 of the European Parliament and of the Council (20) in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the competent supervisory authority.

On October 10, 2022, the European Data Protection Board approved the very first European Data Protection Seal. The certification mechanism encompasses a wide range of data processing operations in many sectors. The "Europrivacy" certification can help data controllers and data processors certify that their data processing is valid in all member states. [127]

[2] Greece-Specific Provisions

In Greece, according to Law 4624/2019, [128] accreditation of certification bodies pursuant to GDPR Art. 42 shall be carried out by the Hellenic Accreditation System (E.S.Y.D.) in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the Hellenic Data Protection Authority. E.S.Y.D. must revoke an accreditation, if informed by the Greek Data Protection Authority that the accreditation requirements are no longer fulfilled, or the certification body is in breach of the GDPR and the provisions of Law 4624/2019.

The Hellenic Data Protection Authority has decided on supplementary requirements for the accreditation of certification bodies; [129] the said requirements are based on the EDPB "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the GDPR" and must be implemented by E.S.Y.D. [130] The Hellenic Data Protection Authority had submitted the draft supplementary criteria for accreditation to the EDPB, pursuant to the consistency mechanism referred to in GDPR Art. 63; the EDPB published Opinion 22/2020 on the draft decision of the competent supervisory authority of Greece regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43(3). [131]

Footnotes

122 GDPR Art. 41(1).

123 GDPR Art. 40(4).

124 https://edpb.europa.eu/system/files/2021-07/edpb_guidelinescodesconducttransfers_publicconsultation_en.pdf.

125 Decision 9/2020; 26/2020.

126 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202020_on_the_el_sa_accreditation_requirements_for_monitoring_body_en.pdf.

127 Opinion 28/2022 on the Europrivacy criteria of certification regarding their approval by the Board as European Data Protection Seal pursuant to Article 42.5 (GDPR)—Adopted on 10 October 2022.

128 Law 4624/2019 Art. 37.

129 Decision 8/2020; Decision 25/2020.

130 "Additional Accreditation Requirements of the Hellenic Data Protection Authority for Certification Bodies in Accordance with Articles 43(1)(b) and 43(3) GDPR in Conjunction with ISO/IEC 17065," *available at* https://www.dpa.gr/sites/default/files/2020- 12/EL_SA_AccreditationRequirementsCB_Rev_EN%28clear%29.pdf.

131 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202022_on_the_el_sa_accreditation_requirements_for_certification_body_en.pdf.

Global Privacy and Security Law - Gilbert, § GRC.15, Greece,NATIONAL DATA PROTECTION LAW—SUPERVISORY AUTHORITY

Francoise Gilbert, Global Privacy and Security Law § GRC.15 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

[A] Overview

[1] GDPR Provisions

Article 51 of the GDPR requires each Member State to set up one or more independent public authorities to be responsible for monitoring the application of GDPR, protecting the fundamental rights and freedoms of natural persons in relation to the processing of their personal data, and facilitating the free flow of personal data within the EU. Each supervisory authority is expected to contribute to the consistent application of the GDPR throughout the EU.

[2] Greece-Specific Provisions

In Greece, the competent authority for the monitoring of application of the GDPR, Law 4624/2019 and other data protection regulation in the Greek territory is the Hellenic Data Protection Authority, a constitutionally consolidated independent public Authority, established by Law 2472/1997 and based in Athens, Greece. [132]

Notably, according to Law 4624/2019, [133] the Hellenic Data Protection Authority is not competent to audit the processing of personal data carried out by judicial and prosecutorial authorities in the context of their judicial function and duties, as well as processing of classified personal data carried out for national safety purposes.

The Hellenic Data Protection Authority has criticized this provision and has highlighted that, while it is not competent to audit the relevant processing of personal data carried out by judicial and prosecutorial authorities, this type of processing remains within the scope of the GDPR. The Authority has also argued that the definition of “classified personal data” can be problematic; therefore, it has suggested that this provision be amended, in order to introduce an obligation of the authorities that process classified personal data to “inform and cooperate” with the Hellenic Data Protection Authority to ensure compliance with the GDPR and adoption of the necessary general safety measures. [134]

[B] Tasks of Supervisory Authorities

[1] GDPR Provisions

GDPR Art. 57 identifies the tasks of supervisory authorities. Among these tasks, the following are especially important for businesses:

- Monitoring and enforcing the application of the GDPR;
- Promoting the awareness of controllers and processor of their obligations under GDPR;
- Informing data subjects concerning their rights;
- Handling complaints lodged by data subjects or entities, investigating the subject matter of a complaint, and informing the complainant of the progress and the outcome of the investigation;
- Cooperating with, and providing mutual assistance to, other supervisory authorities to ensure the consistency of application and enforcement of GDPR;

- Conducting investigations on the application of GDPR;
- Adopting standard contractual clauses;
- Establishing and maintaining a list of requirements for a data protection impact assessment;
- Approving Binding Corporate Rules;
- Contributing to the activities of the European Data Protection Board; and
- Keeping internal records of infringement of GDPR and of measures taken.

[2] Greece-Specific Provisions

In Greece, Law 4624/2019 [135] has introduced additional tasks for the Hellenic Data Protection Authority (expanding those identified in GDPR Art. 57), which *inter alia* include:

- Monitoring and enforcing the application of Law 4624/2019 and other data protection legislation;
- Issuance of Directives and guidelines; and
- Issuance of templates and complaint submission forms.

[C] Investigative Powers of Supervisory Authorities

[1] GDPR Provisions

Article 58(1) of the GDPR defines the investigative powers of supervisory authorities. The following powers are particularly relevant to controllers and processors:

- To order the controller and data processor to provide any information the supervisory authority requires for the performance of its tasks;
- To carry out investigations in the form of data protection audits;
- To review certifications issued by certifying bodies;
- To notify controllers and processors of alleged infringement of GDPR;
- To obtain from the controller and processor access to all personal data and to all information necessary for the performance of its tasks; and
- Obtain access to any premises, including data processing equipment and means, in conformity with EU law or Member State procedural law.

[2] Greece-Specific Provisions

The Hellenic Data Protection Authority, when carrying out investigations and audits, has the power to obtain from the controller and processor access to all personal data processed and all information required for the purpose of the audit and generally for the performance of its duties. No type of secrecy shall apply in such cases against the Authority; [136] as a matter of exception, the Greek Authority may not have access to the identities of partners or employees of entities, which are included in records maintained for national security reasons or for the determination of particularly serious crimes. The members of the Authority competent to conduct such investigations and audits are special investigating officers and have all relevant rights provided by the Greek Criminal Procedure Code.

According to Law 4624/2019, [137] within its investigating powers the Hellenic Data Protection Authority can order the controller and data processor to provide documents, filing systems, equipment or means of personal data processing, and (in certain cases) their contents as well. The Greek Authority may also proceed with seizure of documents, information, filing systems, any equipment and a means of personal data breach, as well as the content thereof; in such case the Greek Authority is appointed as an escrow agent until the competent judicial and prosecutorial authorities reach a relevant decision.

[D] Corrective Powers of Supervisory Authorities

[1] GDPR Provisions

In addition to investigative powers, supervisory authorities have corrective powers listed in GDPR Art. 58(2). Among those corrective powers, the following are noteworthy:

- To issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of GDPR;
- To issue reprimands to a controller or processor where processing operations have infringed provisions of GDPR;
- To order the controller or processor to comply with data subjects' requests to exercise their rights pursuant to GDPR;
- To order a controller or processor to bring processing operations into compliance with GDPR, where appropriate, in a specified manner and within a specified period;
- To order a controller to communicate a personal data breach to the data subject;
- To impose a temporary or definitive limitation, including a ban on processing;
- To order the rectification or erasure of data or restriction of processing, and the notification of such actions to recipients to whom the data have been disclosed;
- Withdraw a certification issued by a certification body, or to order the certification body to withdraw it, or to order a certification body not to issue the certification;
- To impose an administrative fine; and
- To order the suspension of data flows to a recipient in a third country or to an international organization.

[2] Greece-Specific Provisions

In addition to the corrective powers provided for in GDPR Art. 58(2), the Hellenic Data Protection Authority has, under Greek Law 4624/2019, [138] the power to order the controller, processor, or recipient or third party to cease the processing of personal data, or to return or block such data, or to destruct a filing system or relevant data.

[E] Authorization and Advisory Powers of Supervisory Authorities

[1] GDPR Provisions

Under GDPR Art. 58(3), each supervisory authority is granted authorization and advisory powers, in particular, the power to approve BCR and advise controllers in accordance with the prior consultation procedure. They also have an important role in issuing opinions and approving draft codes or conduct and accreditation of certification bodies.

GDPR Art. 58(5) also requires each Member State to provide by law that its supervisory authority has the power to bring infringements of GDPR to the attention of the judicial authorities and, when appropriate, to commence or engage in legal proceedings to enforce the GDPR.

[2] Greece-Specific Provisions

In addition, in Greece, the Hellenic Data Protection Authority may impose the administrative sanctions provided by GDPR Art. 83 and those provided by Law 4624/2019. [139]

[F] Mutual Assistance, Cooperation with Other Supervisory Authorities

GDPR Art. 61 requires that the supervisory authorities provide each other with relevant information and mutual assistance to implement and apply the GDPR in a consistent manner and that they put in place measures for effective cooperation with one another. This mutual assistance covers, in particular, responding to information

requests and implementing supervisory measures, such as requests to carry out prior authorizations and consultations, inspections, and investigations.

There is no additional provision unique to Greece.

[G] Lead Supervisory Authority

Under GDPR Art. 56(1), when a controller or processor operates in several Member States, the supervisory authority of the main establishment of the controller or processor is competent to act as "lead supervisory authority" for the crossborder processing carried out by that controller or processor to handle disputes that involve establishments in several Member States. However, if the subject matter of a dispute relates only to an establishment in its Member State or substantially affects data subjects only in one Member State, the supervisory authority of that member state is competent to handle that complaint. GDPR Art. 56(2).

In cases where a concerned supervisory authority has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned, or where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment, the EDPB shall adopt a binding decision, under its competence as a dispute resolution mechanism, meant to ensure the correct and consistent application of the GDPR in cases involving cross-border processing of personal data. [140]

The same competence is acknowledged to the EDPB by GDPR Art. 65(1), where a competent supervisory authority does not request the opinion of the EDPB or does not follow the opinion of the EDPB, issued under Article 64. In that case, any supervisory authority concerned, or the Commission may communicate the matter to the EDPB. The EDPB has published its "Guidelines 09/2020 on the relevant and reasoned objection of the concerned supervisory authorities," offering guidance on the conditions of such an objection. [141]

There is no additional provision unique to Greece.

Footnotes

132 Law 4624/2019 Art. 9.

133 Law 4624/2019 Art. 10(5).

134 Hellenic Data Protection Authority, Opinion 1/2020, p. 10.

135 Law 4624/2019 Art. 13.

136 Law 4624/2019 Art. 15.

137 Law 4624/2019 Art. 15(4).

138 Law 4624/2019 Art. 15(5).

139 Law 4624/2019 Art. 39.

140 EDPB Guidelines 03/2021 on the application of Article 65(1)(a) GDPR, text *available at* https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_032021_article65-1-a_en.pdf.

141 Text *available at* https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202009_relevant_and_reasoned_obj_en.pdf.

Global Privacy and Security Law - Gilbert, § GRC.16, Greece,NATIONAL DATA PROTECTION LAW—COMPLAINTS, DISPUTES

Francoise Gilbert, Global Privacy and Security Law § GRC.16 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

Data subjects have extensive rights under the GDPR in connection with complaints and disputes.

[A] Right to Lodge a Complaint with a Supervisory Authority

[1] GDPR Provisions

GDPR Art. 77 grants data subjects the right to lodge a complaint with a supervisory authority. If the data subject believes that the processing of his or her personal data infringes the GDPR, he or she may lodge a complaint in the EU Member State where he or she resides, where his or her place of work is, or where the alleged infringement took place. This right is in addition to any other administrative or judicial remedy that an individual might seek.

The supervisory authority with which the complaint has been lodged must inform the complainant on the progress and the outcome of the complaint, including the possibility of a judicial remedy.

[2] Greece-Specific Provisions

In Greece, among the duties of the Hellenic Greek Data Protection Authority, [142] Law 4624/2019 Art. 13 provides for the duty to examine complaints lodged by a data subject or by a body or organization or association, and within a reasonable timeframe to inform the complainant on the progress and the outcome of the investigation or audit.

[B] Right to Effective Judicial Remedy Against Supervisory Authority

[1] GDPR Provisions

GDPR Art. 78 grants data subjects the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. This right is in addition to any other administrative or nonjudicial remedy that an individual might seek.

Data subjects also have the right to an effective judicial remedy when the competent supervisory authority does not handle a complaint or does not inform the data subject on the progress or outcome of the complaint within three months. In these cases, the proceedings against a supervisory authority must be brought before the courts of the Member State where the supervisory authority is established.

[2] Greece-Specific Provisions

In addition, in Greece, Law 4624/2019 [143] identifies judicial remedies against the Hellenic Data Protection Authority (GDPR Art. 78). The Greek Authority's regulatory decisions and individual administrative acts, including the decisions imposing sanctions, may be appealed before the Council of State via a petition for annulment. The deadline for the filing of the petition for annulment does not suspend the execution of the appealed administrative act; upon relevant request by the claimant, the court may (fully or partially) suspend the execution of the act.

[C] Right to an Effective Judicial Remedy Against Controller or Processor

[1] GDPR Provisions

Under GDPR Art. 79, data subjects have the right to an effective judicial remedy against a controller or processor if they consider that their personal data has been processed in non-compliance with GDPR. This right is in addition to their right to exercise any available administrative or nonjudicial remedy, including the right to lodge a complaint with a supervisory authority.

The proceedings against a data controller or a data processor may be brought before the courts of the EU Member State where the data controller or data processor has an establishment or where the data subject has his or her habitual residence.

[2] Greece-Specific Provisions

In addition, in Greece, Law 4624/2019 [144] identifies judicial remedies against a controller or processor (GDPR Art. 79). A data subject's lawsuits against a controller or a processor for breach of GDPR provisions or rights must be filed with the civil court where the controller or the processor has its establishment. Said lawsuits may also be filed with the civil court where the data subject has his/her habitual residence. The above rules do not apply for lawsuits against public authorities, where the said authorities exercise " *sovereign public power*" conferred on them.

When the controller or processor has designated a representative in accordance with GDPR Art. 27(1), such representative will be deemed to be procedural representative for service of documents in the framework of the above-mentioned civil trial.

[D] Right to Mandate Not-for-Profit Organizations to Lodge a Complaint

[1] GDPR Provisions

GDPR Art. 80 grants each data subject the right to mandate certain not-for-profit entities, organizations, or associations to do the following on the data subject's behalf:

- To lodge a complaint;
- To exercise the right:
    - To lodge a complaint with a supervisory authority (under GDPR Art. 77);
    - To have an effective judicial remedy against a supervisory authority that did not handle the data subject's complaint or failed to inform the data subjects on the progress or outcome of the complaint (under GDPR Art. 78);
    - To have an effective judicial remedy against a data controller or data processor; where the data subject considers that his rights have been infringed as a result of the processing of his data (under GDPR Art. 79); and
- To exercise the right to receive compensation from the processor or controller for the damage suffered (under GDPR Art. 82).

To qualify to perform these activities, the not-for-profit entity must have statutory objectives in the public interest and be active in the protection of rights and freedoms with regard to personal data.

Member States may also provide that any not-for-profit entity (within the limits set forth above) may, without having received a mandate from a data subject, lodge in that Member State a complaint with the competent supervisory authority and to exercise the right to an effective judicial remedy against a data controller, data processor, or supervisory authority if that not-for-profit entity considers that the rights of a data subject under the GDPR have been infringed as a result of the processing his or her data.

[2] Greece-Specific Provisions

In Greece, Law 4624/2019 [145] regulates the representation of data subjects (GDPR Art. 80). In case of breach of GDPR provisions or of relevant provisions of Law 4624/2019, the data subject has the right to mandate [146] a not-for-profit body, organization, association or union or a not-for-profit association of persons without a legal personality, which has been lawfully established and operates in Greek territory, which has objectives that are in the public interest and which is active in the field of the protection of data subjects' rights and freedoms with

regard to the protection of their personal data, to lodge before the Hellenic Data Protection Authority a complaint on his or her behalf [147] and to exercise the rights referred to in GDPR Art. 78 and Law 4624/2019 Art. 20.

[E] Right to Compensation; Liability

GDPR Art. 82 grants any person who has suffered damage as a result of an infringement of the GDPR the right to receive compensation from the data controller or data processor for the damage suffered. The rules of allocation of liability, set forth in GDPR Art. 82, include:

- Any controller involved in processing is liable for the damage caused by processing that infringes GDPR.
- Any processor is liable for the damage caused by the processing only if it did not comply with its obligations under GDPR or if it has acted outside, or contrary to, lawful instructions of the data controller.
- A controller or processor is exempt from liability if it proves that it is not responsible for the event giving rise to the damage.
- If more than one controller or processor, or both a controller and a processor, are involved in the same processing and if they are responsible for any damage caused by the processing, they are jointly and severally held liable for the entire damage.
- If a controller or processor has paid full compensation for the damage suffered, it is entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage.
- Proceedings for exercising the right to receive compensation must be brought in the courts of the EU Member State where the case is brought.

There is no additional provision unique to Greece.

Footnotes

142 As specified by Law 4624/2019 Art. 13.

143 Law 4624/2019 Art. 20.

144 Law 4624/2019 Art. 40.

145 Law 4624/2019 Art. 41.

146 By virtue of a special written authorization with certified signature of the mandator.

147 In accordance with GDPR Art. 77.

Global Privacy and Security Law - Gilbert, § GRC.17, Greece,NATIONAL DATA PROTECTION LAW—ADMINISTRATIVE FINES

Francoise Gilbert, Global Privacy and Security Law § GRC.17 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

[A] General Conditions for Imposing Administrative Fines

[1] GDPR Provisions

GDPR Art. 83 grants the supervisory authority the responsibility to ensure that administrative fine for infringements of the GDPR are effective, proportionate, and dissuasive.

Depending on the circumstances, administrative fines are imposed in addition to, or instead of, measures that the supervisory authority may have taken directly, such as ordering an entity to bring processing into compliance or to communicate a breach of security to the data subject.

When deciding whether to impose an administrative fine and its amount, the supervisory authority must take into account the surrounding circumstances, such as:

- The nature, gravity, and duration of the infringement taking into account the nature, scope, or purpose of the processing, the number of data subjects affected, and the level of damage suffered by them;
- Whether the infringement was intentional or negligent;
- Any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- The degree of responsibility of the controller or processor, taking into account technical and organizational measures implemented by them;
- Any relevant previous infringements by the same entity;
- The degree of cooperation with the supervisory authority to remedy the infringement and mitigate the possible adverse effects of the infringement;
- The categories of personal data affected;
- The manner in which the infringement became known to the supervisory authority, in particular whether, and to what extent, the controller or processor gave notice of the infringement;
- If the controller or processor has received prior warning or recommendation from the supervisory authority with respect to the same subject matter, the degree of compliance with those pre-exiting requirements;
- Adherence to approved codes of conduct or certification mechanisms; and
- Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

If an entity intentionally or negligently, for the same or linked processing operations, infringes several provisions of GDPR, the total amount of the administrative fine may not exceed the amount specified for the gravest infringement.

[2] Greece-Specific Provisions

In addition, in Greece, Law 4624/2019 [148] has introduced additional administrative fines specifically against “ *bodies of the public sector*”. Notably, for the purposes of the relevant provision, the term “ *bodies of the public sector*” is more narrowly defined in comparison with the general definition of “public bodies,” which applies in Law 4624/2019.

The Hellenic Data Protection Authority may issue a specifically reasoned decision against the said bodies under their capacity as controllers, after having previously sent an invitation for hearing in order for the controller to be able to offer explanations. More specifically, infringements of:

- GDPR Art. 83(4)(a) (except for GDPR Arts. 8, 27, 29, 42, 43), i.e., the obligations of the controller pursuant to GDPR Arts. 11, 25, 26, 28, 30, 31, 32, 33, 34, 35, 36, 37, 38 and 39;
- GDPR Art. 83(5) and (6), that is, Arts. 5, 6, 7, 9, 12 to 22 (except for Arts. 17 and 20), 44 to 49 (except for Art. 47), any obligations pursuant to Greek law adopted under Chapter IX (except for Arts. 90, 91), 58(2), and 58(1); and
- Law 4624/2019 Arts. 5, 6, 7, 22, 24, 26, 27 (except for par. 7), 28 to 31, 32(1)(a), 33 to 35,

shall be subject to administrative fine up to 10 million Euros.

Law 4624/2019 [149] further describes the factors that the Hellenic Data Protection Authority should take into account when deciding whether to impose an administrative fine and its amount. If the body of the public sector, for the same or linked processing operations, infringes several provisions of the GDPR or Law 4624/2019, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

[B] Amount of Administrative Fines

The GDPR defines two levels of fines, which apply to two categories of offenses.

[1] 10 Million Euros or 2 Percent Annual Turnover Fines

Infringement of the following provisions are subject to administrative fines of up to 10 million euros or up to 2 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- Violation of GDPR Art. 8 regarding the collection of children's personal data;
- Failure to use data processing by design and by default as forth in GDPR Art. 25;
- Failure to designate a data protection officer, if required (GDPR Art. 35); and
- Failure to meet the requirements of a certification body (GDPR Arts. 42, 43).

[2] 20 Million Euros or 4 Percent Annual Turnover Fines

Infringements of other provisions are subject to administrative fines of up to 20 million euros or up to 4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher.

These include, for example,

- Failure to meet the basic principles for processing, including the conditions for consent (GDPR Arts. 5, 6, 7, and 9);
- Infringement of data subjects' rights of information, access to their data, right of rectification, right of erasure, right to restrict the processing of their data, right to data portability, right to object to the processing of their data; right not to be subject to a decision based solely on automated processing, including profiling (GDPR Arts. 12 to 22);
- Failure to comply with the rules pertaining to the transfer of personal data to a third country (GDPR Arts. 44 to 49); and
- Noncompliance with an order or a limitation on processing or the suspension of data flows by the supervisory authority (GDPR Art. 58).

[3] Other Fines and Penalties

In addition, in Greece, Law 4624/2019 [150] has introduced criminal sanctions. More specifically, imprisonment of up to one year (unless the act is punishable more severely by another provision) is provided for anyone who, without right:

- Interferes in any way with a personal data filing system, and by doing so, becomes aware of such data; and
- Copies, removes, alters, damages, collects, records, organizes, structures, stores, adapts, modifies, retrieves, searches for information, associates, combines, restricts, deletes, destroys such data.

Imprisonment of up to five years (unless the act is punishable more severely by another provision) is provided for anyone who, without right uses, transmits, disseminates, shares via transfer, makes available, communicates or makes accessible to unauthorized persons personal data obtained as described under the first point of the above paragraph, or allows unauthorized persons to access such data. If this act relates to special categories of personal data, or data relating to criminal convictions and offenses, or to the security measures referred to in GDPR Art. 10, the offender is to be punished by imprisonment of one to five years and a fine of up to EUR 100.000 (unless the act is punishable more severely by another provision).

Imprisonment of 5 to 10 years is envisaged for the acts described in above paragraphs, if the offender had intended to gain unlawful property benefit for himself or for other person or to cause property damage to another or to harm another, and the total benefit or total damage exceeds EUR 120.000. Imprisonment of 5 to 15 years

and a fine of up to EUR 300.000 is envisaged for the acts described in above paragraphs, if such acts have jeopardized the free functioning of democratic political system or national security.

Footnotes

148 Law 4624/2019 Art. 39.

149 Law 4624/2019 Art. 39.

150 Law 4624/2019 Art. 38.

Global Privacy and Security Law - Gilbert, § GRC.18, Greece,NATIONAL DATA PROTECTION LAW—NOTABLE CASES AND ENFORCEMENT ACTIONS

Francoise Gilbert, Global Privacy and Security Law § GRC.18 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

According to statistics published by the Hellenic Data Protection Authority in May 2020, the total amount of fines imposed by the Authority in the post-GDPR era (covering the period 25 .05.2018–24.05.2020) is EUR 1.565.000; GDPR-related fines amount to EUR 728.000.

Moreover, since May 2018, when the GDPR entered into force, 1996 complaints have been filed with the Authority. Furthermore, data breach incidents notified to the Hellenic Data Protection Authority during the first two years of GDPR enforcement are 247, based on the GDPR, and 49, based on the telecoms regulation.

[A] PricewaterhouseCoopers Business Solutions S.A.

In July 30, 2019, the Hellenic Data Protection Authority published its first Decision exercising the corrective powers conferred on it under the GDPR. This is Decision 26/2019 which imposes a fine of 150,000 on "PricewaterhouseCoopers Business Solutions S.A." (PwC BS) for selection and application of inappropriate legal basis for the processing of employee data and for violation of the principle of accountability. [151] This case set a useful precedent on how a controller and processor can best prepare for an audit by the Hellenic Data Protection Authority and also how they can best deal with such an audit.

The Greek Authority made it clear that where the controller has doubts concerning the lawfulness of the processing, the controller must refrain from processing until compliance is ensured. The Greek Authority highlighted that documentation is a key element of the accountability principle, emphasizing that the authority " *attaches particular importance to the fact that the controller did not provide any evidence of internal compliance which would indicate the documentation of the choice of an appropriate, according to the controller, legal basis* ." In case of non-compliance, corrective measures must be taken as soon as possible and ideally before the conclusion of the audit by the Authority. The Hellenic Data Protection Authority considered as a sanction evaluation factor for deciding of a sanction the fact that the controller had failed to take corrective measures, despite having expressed to the Greek Authority the intention to do so.

[B] Hellenic Telecommunications Organization

In Decisions 31/2019 and 34/2019 of the Hellenic Data Protection Authority, both published in September 2019, administrative fines were imposed on the Hellenic Telecommunications Organization (OTE), a telephone service provider. [152] More specifically:

- In Decision 31/2019, the Greek Authority found that unsolicited calls from third-party companies for the promotion of products and services affected a large number of individual subscribers and imposed a fine of EUR 200.000 for breach of the principles of accuracy [153] and data protection by design. [154]
- In Decision 34/2019, the Hellenic Data Protection Authority found lack of ability to unsubscribe from the list of recipients of advertising messages and imposed an administrative fine of EUR 200.000 for breach of the right to object to the processing for direct marketing purposes [155] and for breach of the principle of data protection by design. [156]

[C] Employment Sector

In its Decision 43/2019 [157] the Hellenic Data Protection Authority found that, in the case of reasonable suspicion of wrongdoing, an employer can have a legitimate interest and right [158] to have access to employee's emails stored on the company's servers. It also pointed out that the employer had relevant policies in place and had informed the employees accordingly.

More specifically, the Hellenic Data Protection Authority argued that an employer, exercising its managerial right to protect the property and the proper functioning of the company, [159] has the right to exercise control over the electronic media it provides to its employees for performing their duties within the scope of the company's business operations, [160] provided that the employees are adequately informed about relevant processing.

The Hellenic Data Protection Authority stated that an employer's legitimate interest can *inter alia* be the safeguarding of know-how, confidential information and trade secrets, ensuring the proper functioning of the business and obtaining confirmation or proof of the criminal activities conducted by an employee. The Hellenic Data Protection Authority further argued that the employee's use of networks, electronic communications systems or data storage media owned by the employer, for which the employee has previously been explicitly informed that are available for professional/ business use only, does not as such (i.e., without reasonable suspicions) constitute a legitimate reason for constant monitoring. However, *ad hoc* and targeted monitoring would be acceptable where there is reasonable suspicion of an unlawful act, internal policies are in place prohibiting use of electronic communications systems and media for personal/ non-business purposes, and the employees have been informed about such prohibition and also about the employer's ability to access to the electronic communications systems and media in question.

The Hellenic Data Protection Authority also noted that monitoring of employees and access to their data stored on employer's systems and devices, without prior notice to employees, cannot be *a priori* excluded; it can exceptionally take place under the condition that such monitoring and access is either provided or not prohibited by law, and provided that the necessary measures have been taken for access to professional electronic communications. [161] Even when no internal policy is in place and no prior notice has been given to employees, access to employee's emails stored on an equipment belonging to the employer, such as a computer or server can be acceptable, in case of a "compelling force majeure" and in compliance with the principle of proportionality. [162]

[D] Data Subjects' Rights

The Hellenic Data Protection Authority has examined a series of cases concerning the failure of data controllers to satisfy data subjects' rights. Notably:

- A fine of EUR 8,000 has been imposed on a data controller for breach of the data minimization principle, also for not responding to (essentially silently rejecting) a data subject's request to receive a copy of video material that concerned him. The data controller, former employer of the complainant, had been requested by the former employee to issue a document certifying employment with the said employer; the latter deemed appropriate to include in the said document, apart from the type of and duration of

employment, also the fact that former employee had been fired due to a criminal offence. The Hellenic Data Protection Authority deemed that, in the context discussed, this additional information is not relevant or necessary and, as such, it should not be included in a certificate of employment. [163]

- The Hellenic Data Protection Authority examined the request of a data subject to access the communication between a trader and a bank regarding his transaction as consumer, due to the fact that monthly instalments continued to be paid despite the fact that the purchased product had been returned to the trader. The trader refused to grant access and the bank did not respond to the request. The Hellenic Data Protection Authority considered the submission of the relevant request via the Messenger app as being appropriate. The Hellenic Data Protection Authority deemed both, the trader and the bank, in breach of Article 15 of GDPR and imposed a fine of EUR 20,000 to each one of them. [164]
- A fine of EUR 5,000 has been imposed on a data controller due to continuous failure to delete a data subject's personal data from its website. The data controller administers a website with a public registry of doctors. A doctor included in the said registry requested twice that her personal data are removed from the said registry; the data controller did not provide any response. The Hellenic Data Protection Authority deemed processing unlawful, in breach of Articles 5(1)(a) and (e) and 6(1) of GDPR, while ascertaining the lack of conformity with the obligation to satisfy the data subject's rights. [165]
- The Hellenic Data Protection Authority examined the complaint of a father, who requested access to his underage child's personal data. The data controller maintains a facility offering recreational activities to children; the child had been enrolled by the mother. The father, exercising his parental responsibility, requested access to personal data of his child. The data controller did not satisfy the request, even though the Hellenic Data Protection Authority had specifically ordered the access. The total fine imposed amounted to EUR 8,000 for failure to satisfy the right of access and comply with the Hellenic Data Protection Authority's order. [166]
- The Hellenic Data Protection Authority examined the complaint of a data subject, who had requested the erasure of his personal data by a data controller, a retailer. The data controller initially did not respond to the request, however following the intervention of the Hellenic Data Protection Authority, the data controller declared that the information of the complainant had been deleted. Soon after, the complainant received marketing communication (SMS) from the same data controller. The Hellenic Data Protection Authority imposed a fine of EUR 20,000 for failure to satisfy the data subject's data erasure request. [167]
- The Hellenic Data Protection Authority examined the complaint of a data subject against her employer for failure to satisfy her right to object, regarding the possibility of continuous monitoring by the former of the online courses provided by the complainant through the online platform "zoom." The Authority found that the employer did not satisfy the above right of objection and that the legal basis of the contested processing was not clearly satisfied, thus imposing a fine of EUR 2,000. [168]
- The Hellenic Data Protection Authority examined the complaint of a consumer against a bank for a personal data breach incident, consisting of the transmission of bank alerts to a third party, containing the complainant's full name, despite the consumer's prior notification to the bank. The Authority imposed a fine of EUR 10,000 due to the breach of the principle of confidentiality, as well as for the failure to notify the Authority and the subject of the incident. Moreover, a warning was issued to the bank in relation to the inadequate and organizational security measures, meaning the absence of measures to confirm the e-mail addresses declared for the purpose of sending bank alerts. [169]

[E] COSMOTE—Mobile Telecommunications Single Member S.A.

Following the notification of a personal data breach incident by COSMOTE, covering the leakage of subscriber call data in the period between September 1, 2020 and September 5, 2020, the Hellenic Data Protection Authority investigated the circumstances under which the incident took place and, in this context, examined the legality of the maintenance of the leaked records and the security measures applied.

The leaked file contained subscribers' traffic data retained for the purpose of managing technical problems for 90 days from the making of calls and further, the data of the leaked file were pseudonymized and retained for 12 months, for statistical purposes, such as the optimization of the design of the mobile telephony network, after being enriched with additional simple personal data.

The Hellenic Data Protection Authority imposed a fine for a total amount of EUR 6,000,000, as well as a sanction of interruption of processing and destruction of data, for the infringement of the principles of lawfulness and transparency due to the provision of unclear and incomplete information to the subscribers. Also, the Hellenic Data Protection Authority noted that the company failed to carry out the necessary data processing impact assessment, as well as to implement the appropriate security measures.

During 2022, proceedings against COSMOTE were brought twice before the Hellenic Data Protection Authority. In the first case, the company faced an administrative fine of EUR 150,000 for the lack of appropriate technical and organizational measures to protect the security of their services. The Authority identified a series of data protection and privacy legislation violations, such as failure to ensure the security of data processing, consisting in failure to demonstrate compliance with their policies or lack of adequate policies. [170]

In the second case, COSMOTE and its affiliate Hellenic Telecommunications Organization (OTE) faced a total administrative fine of EUR 9,250,000 due to the infringement of the principles of legality and transparency, as well as due to unclear and incomplete information provided to subscribers, inadequate security measures, incorrect implementation of anonymizing procedures, failure to identify and allocate processing roles between the companies of the group. Further, they demonstrated inadequate security measures in place with regard to the infrastructure used in connection with a data breach incident. [171]

[F] Clearview AI Inc—Facial Recognition Software Company

Following a complaint filed by the NGO “Homo Digitalis” in May 2021 representing a data subject, the Hellenic Data Protection Authority issued Decision 35/2022 [172] imposing a fine of EUR 20,000,000 million on Clearview AI for violating the principles of lawfulness and transparency.

In addition, the Hellenic Data Protection Authority ordered the company to comply so that it satisfies the complainant’s request for access to personal data, while imposing a prohibition on the collection and processing of personal data of subjects located in the Greek territory, using methods included in the facial recognition service. Finally, with this decision, the Hellenic Data Protection Authority ordered Clearview AI to delete the personal data of those subjects located in Greece, which they collected and processed in violation of data protection legislation.

The administrative fine imposed on Clearview AI is a record fine for the Hellenic Data Protection Authority.

Footnotes

151 An official summary of Decision 26/2019 is available at https://www.dpa.gr/pls/ portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/SUMMARY%20OF%20DECISION%2026_2019%20(EN).PDF.

152 An official summary of Decision 26/2019 is available at https://edpb.europa.eu/ news/national-news/2019/administrative-fines-imposed-telephone-service-provider_en.

153 GDPR Art. 5(1)(c).

154 GDPR Art. 25.

155 GDPR Art. 21(3).

156 GDPR Art. 25.

157 An official summary of the Decision 43/2019 is available at https://edpb.europa. eu/news/national-news/2020/investigation-regarding-access-and-inspection-employer- employees-emails_en.

158 Under GDPR Art. 5(1) and 6(1)(f).

159 Subject to the condition of compliance with the principles of GDPR Art. 5(1).

160 To the extent that such processing is in accordance with the principle of proportionality, and is necessary for the purposes of the legitimate interests pursued by the employer and provided that the interests of the employer clearly override the interests, fundamental rights and freedoms of the employees.

161 Article 29 Working Party, Working document on the surveillance of electronic communications in the workplace (WP 55), adopted on 7 June 2012, *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf ; International Labor Organization, Protection of workers' personal data (Code of practice), 1997, *available at* https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf.

162 Decision 37/2007 of the Hellenic Data Protection Authority.

163 Decision 39/2021 of the Hellenic Data Protection Authority.

164 Decision 36/2021 of the Hellenic Data Protection Authority.

165 Decision 37/2021 of the Hellenic Data Protection Authority.

166 Decision 29/2021 of the Hellenic Data Protection Authority.

167 Decision 13/2021 of the Hellenic Data Protection Authority.

168 Decision 12/2022 of the Hellenic Data Protection Authority.

169 Decision 6/2022 of the Hellenic Data Protection Authority.

170 Decision 39/2022 of the Hellenic Data Protection Authority.

171 Decision 4/2022 of the Hellenic Data Protection Authority.

172 Decision 35/2022 of the Hellenic Data Protection Authority.

Global Privacy and Security Law - Gilbert, § GRC.19, Greece,CUSTOMER TRACKING; COOKIES

Francoise Gilbert, Global Privacy and Security Law § GRC.19 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

[A] Laws Governing the Use of Cookies

The use of cookies is regulated by Law 3471/2006 Art. 4 (as amended by Law 4070/2012 Art. 170), which has transposed the EU Cookies Directive (2009/136/EC). The storage of information on or the access to information already stored on a device is permitted only if the user of the device has provided informed consent. Such consent can be expressed by using the appropriate settings of a browser or other application. The above does not prevent any technical storage or access for the sole purpose of carrying out a transmission of a communication over an electronic communications network or any technical storage or access that is necessary for the provision of an information society service, which has been explicitly requested by the user.

[B] Hellenic Data Protection Authority's Guidance Regarding Cookies

The Hellenic Data Protection Authority has published on its website Guidelines on Use of Cookies attempting to further explain the relevant provision. They refer to exceptions where no consent is required, essentially reproducing the Article 29 Working Party Opinion 04/2012 on Cookie Consent Exemption (WP194). [173]
Said exceptions are: "user-input" cookies, user-centric security cookies, multimedia player session cookies,

authentication cookies, user interface customization cookies, load-balancing session cookies, and social plug-in content-sharing cookies. Special reference is also made to web analytics cookies and online advertising cookies (first- and third-party cookies), which according to the Guidelines on Use of Cookies are not included in the above exceptions and therefore prior consent is required. The Hellenic Data Protection Authority recognizes the need to further review and discuss the issue of web analytics cookies. It is also noted that a user-friendly mechanism to opt-out must be in place.

Footnotes

173 Article 29 Working Party, Opinion 04/2012 on Cookie Consent Exemption (WP 194), adopted on 7 June 2012, *available at* https://ec.europa.eu/justice/article-29/ documentation/opinion-recommendation/files/2012/wp194_en.pdf.

Global Privacy and Security Law - Gilbert, § GRC.20, Greece,DIRECT MARKETING

Francoise Gilbert, Global Privacy and Security Law § GRC.20 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

Direct marketing communications are primarily regulated by Law 3471/2006, [174] GDPR provisions, Article 29 Working Party Guidelines on consent under the GDPR [175] and Hellenic Data Protection Authority Opinion 2/2011 on electronic consent.

[A] Marketing by E-Mail/SMS

In principle, marketing by e-mail/SMS requires the recipient's prior consent (opt-in). A limited exception to the above consent requirement applies (soft opt-in), which can solely be used if all the following apply:

1. The respective email address/telephone number has been obtained from the recipient/ customer in the context of the sale of a product or a service or other “transaction”; [176]
2. The email address is used for direct marketing of own similar products or services or purposes;
3. The recipient/ customer has been clearly and distinctly given the opportunity to object, free of charge and in an easy manner, when the email address had been collected and on the occasion of each email; and
4. The customer has not objected to such emails.

The controller should ensure that it uses clear and plain language. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form. That said, a declaration by the user that she/he has been informed (e.g., by ticking a relevant box) will not be sufficient when notice is not actually easily accessible (e.g., this would be the case when the notice is accessible only via a hyperlink leading to another page).

When consent is to be given by electronic means, the request must be clear and concise. According to the Article 29 Working Party, layered and granular information can be an appropriate way to deal with the two-fold obligation of being precise and complete on the one hand and understandable on the other hand. Same applies for mobile interfaces; to accommodate for small screens or situations with restricted room for information, a layered way of presenting information can be considered, where appropriate, to avoid excessive disturbance of user experience or product design.

Further, according to guidance by the Hellenic Data Protection Authority, when consent is provided via a website, notice can be provided for instance by (a) making/ “forcing” the user to read the notice (via a pop-up window) before being able to provide consent, or (b) placing notice on a special field or adequate size and making/ “forcing” the user to scroll down the text before being able to provide consent. JavaScript code can be used in order for controller to be able to control and prove that the user has actually read the notice before giving his/her consent.

The GDPR clearly outlines the explicit obligation of the controller to demonstrate a data subject's consent; the burden of proof will be on the controller. It is up to controller to prove that valid consent was obtained from the data subject and to this end the controller is free to develop methods to comply with this provision in a way that is fitting in its daily operations. However, the GDPR does not prescribe exactly how this must be done.

According to Article 29 Working Party, as long as a data processing activity (marketing in this case) lasts, the obligation to demonstrate consent exists. After the processing activity ends, proof of consent should be kept no longer than strictly necessary for compliance with a legal obligation or for the establishment, exercise or defense of legal claims. According to Hellenic Data Protection Authority, a record of receiving consent (and withdrawal of consent) must be retained up to six months as of last communication activity or withdrawal of consent.

GDPR prescribes that the controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time (this does not mean though that giving and withdrawing consent must always be done through the same action). When consent is obtained via electronic means through only one mouse-click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that consent equally as easily. Where consent is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, or by e-mail), a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort. It is highlighted that the requirement of an easy withdrawal is a necessary aspect of valid consent in the GDPR, meaning that if the withdrawal right does not meet the GDPR requirements, then the consent mechanism of the controller does not comply with the GDPR.

According to the Data Protection Authority Opinion 2/2011 on electronic consent, the controller must make sure that consent is recorded in a way that ensures technical proof of (a) the provision of consent and (b) the fact that the user has access to the provided email address/SMS.

[B] Marketing by Telephone

Direct marketing by telephone without human intervention (i.e., automated calls) requires prior informed consent (opt-in).

However, marketing by telephone with human intervention is in principle permitted, unless the recipient has opted out from such communication (opt-out). Currently, there is no national “do not call” registry in Greece; each telecom provider is obliged to maintain its own registry with subscribers who have opted out from receiving such marketing communications. Before an individual is contacted by telephone it must be ensured that the said individual is not included in the said opt-out registries.

The Hellenic Data Protection investigated a series of complaints for data controllers who proceeded in direct marketing without adhering to their legal obligations under Article 11 of Law 3471/2006. The investigations concluded with the imposition of fines ranging between EUR 25.000 to EUR 30.000 per controller. Notably, the Data Protection Authority commented that in addition to the fact that the controllers had not demonstrated that they obtained consent, the very process they had followed did not ensure that valid consents are obtained. [177]

[C] Marketing by Postal Mail

Postal mail communication (printed promotional material) can be established only (a) with recipients who have provided their prior consent (opt-in), or (b) in cases when the controller has obtained the contact information in

the framework of a previous business relationship with the recipient, or (c) when the recipient's data are collected from a legitimate source (e.g., telephone directories).

In both above cases (b) and (c) the controller/sender must ensure that the recipient has not previously objected to such communication, e.g., the recipient is not included in the opt-out list, the so called "Article 13 registry," maintained by the Hellenic Data Protection Authority.

[D] Data Processing for the Purpose of Political Communication

The Hellenic Data Protection Authority has published "Guidelines 1/2019 on data processing for the purpose of political communication," specifying data protection rules on political marketing via any means and at all times, including the pre-election period. The Guidelines cover political parties, members of the Greek and European Parliament, political organizations and, generally, elected individuals and candidates in any kind of elections; they also cover different types of communication, including telephone calls with human intervention, as well as use of electronic means without human intervention (e.g., SMS, MMS, e-mails, messaging apps, automated telephone calls with pre-recorded messages and voice messages via automated voicemail).

Also, the Hellenic Data Protection Authority has published Opinion 7/2021 on the access by candidates in the Athens Bar Association elections to the contact details of the Bar Association's member lawyers. In this Opinion, the Authority maintained that the provision of such contact details to candidates is compatible with the data protection legislation, assuming that the legal basis of the processing is Article 6(1e') of the GDPR, i.e., public interest in the functioning of the Bar Association and in the conduct of elections in a manner that ensures the visibility of the positions of all candidates. It was also stated that even though the subjects had not been informed at the collection stage, there may be an application of Article 6(4) GDPR, as the purpose is relevant to the original purpose.

The Hellenic Data Protection Authority has dealt with a series of cases concerning the unlawful processing of personal data for the purpose of political communication; indicatively, fines for unsolicited communication (spamming) of EUR 2,000 (per case) have been imposed on a candidate in municipal elections of May 2019, also on candidates in parliamentary elections of July 2019. [178]

By decisions 1343-1344-1345/2022 of the 4th Chamber, the Council of State annulled decisions 13/2020, 10/2020 and 11/2020 of the Hellenic Data Protection Authority, respectively, by which administrative fines had been imposed on parliamentary candidates for unlawful processing of personal data for the purpose of political communication through e-mails. The Council of State deemed that political communications do not fall under the scope of unsolicited communications as per Art. 11 par. 1 of Law 3471/2006, and posited that special rules are required in order to limit such political communications, necessary for the functioning of a democratic society, between candidates and voters during the election period.

Taking into account the above-mentioned decisions of the Council of State, the Hellenic Data Protection Authority estimated that there is a legitimate reason to revoke any contrary previous decisions, which imposed sanctions based on the provision of Article 11 of Law 3471/2006 and not on the provisions of the GDPR, which continues to apply for the assessment of the lawfulness of any processing.

Footnotes

174 Implementing Art. 13(2) of Directive 2002/58/EC.

175 Article 29 Working Party, Guidelines on consent under Regulation 2016/679 (WP259 rev.01), adopted on 28 November 2017, as last revised and adopted on 10 April 2018, *available at* file:///Users/tedio/Downloads/20180416_Article29WPGuidelineson Consent_publishpdf.pdf.

176 It is noted that legal definition of "transaction" is a vague issue under applicable legislation.

177 Decisions 52/2021, 56/2021, and 57/2021 of the Hellenic Data Protection Authority.

178 Decisions 07/2021, Decision 08/2021, 09/2021 and 19/2021 of the Hellenic Data Protection Authority.

Global Privacy and Security Law - Gilbert, § GRC.21, Greece,TELECOMMUNICATIONS SECTOR

Francoise Gilbert, Global Privacy and Security Law § GRC.21 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

According to the General Authorization Regulation governing the licensing framework for electronic communications in Greece, providers of electronic communication networks and/or services must comply with the applicable provisions on the protection of personal data, the confidentiality of communications and the protection of privacy in electronic communications. [179] Any agreement to limit or exempt the provider's liability under the above provisions shall be null and void.

The obligations on providers of electronic communication networks and/or services concerning matters of privacy and secrecy are monitored by the Authority for the Information and Communication Security and Privacy ("ADAE"), a constitutionally consolidated independent Authority, with a mission to ensure the confidentiality of mail and all other forms of free correspondence or communication.

In accordance with the legislation for the secrecy of electronic communications and in particular Regulation for the Assurance of Confidentiality in Electronic Communications [180] by ADAE, all persons providing electronic communication networks and/or services are obliged to apply a *Security Policy for the Assurance of Communications Confidentiality* (the "Policy"), which must be filed with and approved by ADAE.

The Policy must define the following:

- Acceptable Use Policy;
- Physical Security Policy;
- Logical Access Policy;
- Remote Logical Access Policy;
- ICS Management and Installation Policy;
- Security Incident Management Policy;
- Network Security Policy;
- Audit Policy for the Implementation of the Security Policy for the Assurance of Communications Confidentiality;
- Anti-Malware Policy; and
- Encryption Policy.

The provider must appoint an employee as the *Communications Confidentiality Assurance Officer* , who is responsible for control of the implementation of the measures and requirements laid down in the Policy.

The provider is obliged to define in the Policy and implement measures and/or procedures relating to the use, dispatch, and destruction of storage media, which contain communications data or other information which could lead to the disclosure of communications data of subscribers or users of the networks or services provided (such as access codes and ICS structural data), so as to prevent them from being disclosed to non-authorized persons, to take all necessary and adequate measures to physically protect the facilities, so as to prevent all unauthorized access to them and to control physical access so that access is only permitted to authorized persons and designate secure areas within its facilities where ICS are installed. These areas must be protected by robust security mechanisms (i.e., direct detection systems for unauthorized access and CCTV) and controlled access systems (i.e., controlled entry cards) in compliance with the relevant legislation.

For *providers of public communication networks or public electronic communication services* , [181] the applicable rules are found in the Regulation for the Safety and Integrity of Networks and Electronic Communications Services, issued by ADAE [182] and the Joint Act 1/2013, issued by ADAE and the Hellenic Data Protection Authority. The Regulation for the Safety and Integrity of Networks and Electronic Communications Services defines the technical and organizational measures that need to be implemented by the said providers to ensure data security, including reference to business impact analysis, business continuity, penetration tests, vulnerability assessments, physical security, backups, power management, logical access controls, security zones, firewalls, VPNs, intrusion detection systems, event logging, security incident management. It also introduces an obligation regarding the collection and retention of certain information in case of data breaches involving over 500 users and with duration over one hour. Further, the Joint Act 1/2013 includes also data safety guidelines in the context of the data retention obligations imposed by Law 3917/2011 on the said providers and refers to the technical and organizational measures that need to be implemented in order to ensure data security; measures include the appointment of a Data Security Officer, data separation, business continuity, physical security, backups, logical access controls, security zones, event logging, security incident management, data destruction policy, internal controls, and data encryption. Non-compliance with the Regulation for the Safety and Integrity of Networks and Electronic Communications Services can be punished with imprisonment up to five years and fine up to EUR 60,000.00.

Footnotes

179 Decision 991/4 (/17.05.2021) by the Hellenic Telecommunications and Post Commission (EETT), as in force.

180 Regulation 165/2011 (17.11.2011); available in EN at http://www.adae.gr/file admin/docs/nomoi/kanonismoi/ADAE_REGULATION_165.2011.pdf.

181 As defined in Law 4727/2020 (same definition also used in Law 3471/2006): Article 110(A.39) of Law 4727/2020 on electronic communications defines " *electronic communications services* " as

> *(…) services usually offered upon remuneration over electronic communications networks and the provision of which includes (with the exception of services which provide content transmitted using electronic communications networks and services or which exercise control over content) the following services:*
>
> *(a) "internet access service" as defined in Article 2 of Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures on open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) 531/2012 on roaming on public mobile communications networks within the Union,*
>
> *(b) interpersonal communications services; and*
>
> *(c) services consisting, in whole or in part, in the transport of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting.*

182 ADAE Decision 205/2013 (as amended by ADAE Decision 99/2017).

Global Privacy and Security Law - Gilbert, § GRC.22, Greece,EMPLOYEE INFORMATION

Francoise Gilbert, Global Privacy and Security Law § GRC.22 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

[A] General Rules Governing Employee Information

Law 4624/2019 [183] regulates data processing in the context of employment. Processing of employees' personal data is permitted for the purposes of the employment agreement, "if absolutely necessary for the decision to conclude the employment agreement, or after conclusion, for its performance."

[1] Exceptional Use of Consent

In case where processing is exceptionally based on employee's consent, when assessing whether consent is freely given, mainly the following factors must be considered:

- "The dependence of the employee" according to the employment agreement, and
- The circumstances under which consent has been provided. Consent can be provided electronically or in writing and clearly separately from the employment agreement.

As highlighted by the Hellenic Data Protection Authority, [184] the exceptional use of consent as the legal basis for the collection of personal data in the context of employment relationship could be compliant with the GDPR only if (a) the use of any other legal basis provided by GDPR Art. 6(1) is not possible, due to the relevant circumstances [185] and (b) the GDPR requirements of a valid consent [186] are fulfilled. By derogation from of GDPR Art. 9(1), processing of special categories of personal data for the purposes of the employment agreement is permitted, "if necessary for the exercise of rights or for carrying out legal obligations in the field of employment, social security and social protection law and there is no reason to deem that processing is overridden by the legitimate interests of the data subject."

As noted by the Hellenic Data Protection Authority, [187] this is essentially a repetition of GDPR Art. 9(2)(b) without providing for "appropriate safeguards for the fundamental rights and the interests of the data subject" [188] or "suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity." [189]

Processing of employees' personal data (including special categories of personal data) is also permitted on the basis of collective labor agreements.

[2] Use of CCTV

Processing of employees' personal data via CCTV, which is installed in the working areas, regardless of whether such areas are publicly accessible or not, is permitted " *only if required for the protection of persons and goods* ." Such data may not be used for the evaluation of the employees' productivity. The employees must be informed in writing (on paper or electronically) for the installation and operation of a CCTV system in the working areas.

[3] Definition of "Employee"

It is being clarified that under the definition of "employee"' any individuals employed under any type of employment or service provision, irrespective of the validity of the agreement, also including job applicants and former employees would be encompassed in the term "employee."

The above rules, as introduced by Art. 27 of Law 4624/2019, have been criticized by the Hellenic Data Protection Authority. [190] More specifically, in the explanatory report of Law 4624/2019 (as filed with the Parliament) the performance of the employment contract [191] is noted, for example, as the legal basis for the (i) processing of employees' biometric data, (ii) use of geolocation systems, (iii) introduction of company rules on the use of communications and electronic surveillance media, and (iv) implementation of whistleblowing schemes.

This approach has been heavily criticized by the Hellenic Data Protection Authority, [192] arguing that the performance of the employment contract in not an appropriate legal basis for the above data processing operations, whereas the legitimate interests pursued by the employer [193] would be a more suitable legal basis, as also argued in a number of decisions issued by the Hellenic Data Protection Authority in the previous years. [194]

[B] Rules Applying to Biometric Information in the Employment Context

In the context of employment, the use of biometric methods for identification and access control purposes can be permissible only when this is required due to special safety requirements (e.g., in high-risk laboratories or high security facilities [195]) and where, at the same time, there is no other, less privacy intrusive means to achieve said purpose.

In a number of instances, the Hellenic Data Protection Authority has found the use of biometric systems and methods to be disproportionate to the data privacy risks posed and, as such, inappropriate and in breach of applicable data protection rules and principles. [196]

[C] Rules Applying to Geolocation Information in the Employment Context

The Hellenic Data Protection Authority has, in a number of occasions, examined the use of geolocation technologies in an employment context; most recently in Decision 37/2019. The Authority has adopted the Article 29 Working Party Opinion on the use of location data with a view to providing value added services, [197] arguing that data processing that allows an employer to collect data on the location of an employee, either directly (location of the employee him/herself) or indirectly (location of the vehicle used by the employee or of a product or asset in his/her charge) involves the use of personal data and is subject to the provisions of applicable data protection legislation. Geolocation can very often provide further information on the data subject's habits and preferences, potentially allowing for the creation of behavioral profiles. The legality of such data processing is examined on the basis of the principles of GDPR Art. 5 and generally the principle of proportionality; [198] in addition, data subjects must have been properly informed. [199]

The lawfulness of such processing operations should not rely exclusively on the employee's consent, which must be "freely given" and as a legitimate ground for processing is (in most cases) problematic in an employment context. [200] As argued by the Article 29 Working Party [201] and the Hellenic Data Protection Authority:

> *Instead of seeking consent, employers must investigate whether it is demonstrably necessary to supervise the exact location of employees for a legitimate purpose and weigh that necessity against the fundamental rights and freedoms of the employees. In cases where the necessity can be adequately justified, the legal basis of such a processing could be based on the legitimate interest of the employer, who must always seek the least intrusive means, avoid continuous monitoring and for example choose a system that sends an alert when an employee is crossing a pre-set virtual boundary. An employee must be able to turn off any monitoring device outside of work hours and must be shown how to do so .*

Processing based on the legitimate interest of the employer could include monitoring of the transportation of people or goods, or the improvement of the distribution of resources for services in dispersed areas, or in order to ensure safety of the employee or the goods or the vehicles entrusted to employees. [202]

On the other hand, processing of personal data through a geolocation system is considered to be excessive, when employees are not free to organize the details of their journey, or when such processing takes place exclusively for monitoring of the employee's work, when such monitoring can be performed with milder means. In

any case, such processing must not take place outside working hours, while employers should not use tracking devices in order to locate or monitor the behavior or location of drivers or other staff members. [203]

Lawful use of a geolocation system requires that the employee follows a predetermined route within specified working hours, geolocation takes place within the said predetermined route and the employee does not use the vehicle outside of working hours. [204] Employees must be adequately informed in compliance with GDPR Arts. 13 and 14. Such notice must be individually provided to each employee, while the employer must be in a position to prove "in a reasonable way" that notice has been provided. [205]

[D] Processing of Employees' Personal Data in the Context of the COVID-19 Outbreak

On March 18, 2020, the Hellenic Data Protection Authority published Guidelines in the context of the COVID-19 outbreak, according to which, employers (controllers) can proceed with " *necessary and appropriate data processing activities in accordance with GDPR Arts. 5 and 6 (…), while no data processing activity can a priori be excluded, in particular under the current unprecedented situation.* " Further, as noted by Hellenic Data Protection Authority, measures which are onerous and constitute a limitation of individuals rights (e.g., temperature checks) must be used as a last resort and " *after any available appropriate measure has been previously excluded.* " Notably, the Authority highlights that " *a systematic, continuous and generalized collection of personal data that leads to establishment and continuous update of employee health profiles, could hardly be described as compliant with the principle of proportionality.* "

According to currently applicable legal framework, employees who have completed COVID-19 vaccination or have been affected by COVID-19 within the past six months, in order to enter work premises, are obliged to demonstrate to the employer an EU Digital COVID Certificate (EUDCC), or a vaccination certification (issued by the Greek State), or a certificate of a positive COVID-19 test, or an equivalent certificate or certification issued by a third country. [206] Unvaccinated employees, in order to enter work premises, need to present a negative Rapid or PCR test per week. The employer has the right and obligation to review the information concerning the weekly test results of its employees, meaning the full name of unvaccinated employees, the method of testing, the test result and the week of reference. [207] Such information is automatically uploaded by the private laboratories (or hospitals, private practitioners, etc.) to the National Covid-19 Registry, which, in turn, automatically shares this information with the online employment platform "ERGANI."

Currently, there is no statutory provision or official guidance by Greek authorities specifically on the use of contact tracing devices. However, the Hellenic Data Protection Authority on its website also refers to relevant material and guidance produced by the European Parliament, [208] the European Commission, [209] the eHealth Network, [210] the European Union Agency for Fundamental Rights, [211] the European Data Protection Board, [212] the European Data Protection Supervisor, [213] the Global Privacy Assembly, and the Council of Europe, which include references to contact tracing devices and apps.

The Hellenic Data Protection Authority has also published Guidelines on security measures in the context of teleworking, raising awareness of controllers, processors, and data subjects on the relevant risks and the obligations imposed by the GDPR and Law 4624/2019. The said Guidelines include certain technical and organizational measures, mainly covering network access (e.g., suggested use of IPSec VPN, WPA2), use of e-mail and messaging applications (e.g., avoid use of third-party email services, encryption), use of terminal devices and storage media (e.g., firewall, make software updates, data segregation, use of virtual machine, encryption, and backup copies), and teleconferencing (e.g., use of platforms and software that support end-to-end encryption).

Footnotes

183 Law 4624/2019 Art. 27.

184 Hellenic Data Protection Authority, Opinion 1/2020, p. 18.

185 Especially the legal basis of GDPR Art. 6(1) (b), (c) and (f)

186 Per GDPR Art. 4(11) and GDPR Art. 7.

187 Hellenic Data Protection Authority, Opinion 1/2020, p. 18-19.

188 As required by GDPR Art. 9(2)(b)

189 As required by GDPR Art. 88(2)

190 Hellenic Data Protection Authority, Opinion 1/2020, p. 16-19.

191 *See* GDPR Art. 6(b)

192 Hellenic Data Protection Authority, Opinion 1/2020, p. 16-17.

193 Per GDPR Art. 6(f)

194 Indicatively, Decision 37/2019 on use of geolocation technologies; Decision 34/2018 on access to employee's computer; Decisions 43/2019 and 44/2019 on access to server with stored employee data; Decision 26/2019 on monitoring of employee's electronic communications.

195 Decision 56/2009 of the Hellenic Data Protection Authority, where the Authority permitted the use of a biometric system by a provider of electronic signature certification services, in order to control personnel access to certain high security facilities/areas.

196 Decision 59/2005 of the Hellenic Data Protection Authority rejecting the installation of a pilot biometric system for access control to sports facilities; Decision 62/2007 of the Hellenic Data Protection Authority rejecting the installation of a biometric system for access control to working areas; Decision 245/9/2000 of the Hellenic Data Protection Authority which found illegal the use of fingerprints by Municipal Authority to control access of employees to working areas.

197 Article 29 Working Party, Opinion on the use of location data with a view to providing value added services (WP 115), November 2005, *available at* https://ec.europa. eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf.

198 Processing must be suitable and necessary in relation to the intended purpose, which cannot be achieved by milder and equally effective means.

199 ECJ C-201/14: Smaranda Bara.

200 As pointed out by the Article 29 Working Party, the issue of consent should be addressed in a broader perspective; in particular, the involvement of all the relevant stakeholders via collective agreements might be an appropriate way to regulate the gathering of consent statements in such circumstances.

201 Article 29 Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices (WP 185), 16 May 2011, *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf.

202 Decisions 162/2014, 163/2014 and 165/2015 of the Hellenic Data Protection Authority.

203 As highlighted by Article 29 Working Party, " *vehicle tracking devices are not staff tracking devices. Their function is to track or monitor the location of the vehicles in which they are installed. Employers should not regard them as devices to track or monitor the behaviour or the whereabouts of drivers or other staff, for example by sending alerts in relation to speed of vehicle* " (Opinion 13/2011).

204 For instance, the Hellenic Data Protection Authority approved the use of GPS technology installed in the garbage trucks of the Municipality of Piraeus, under the condition that the vehicles follow a predetermined route and geolocation is used for route optimization purposes only and not in order to monitor employees (Decision 163/2014).

205 Data retention should not be longer than what is absolutely required for the needs of the processing in question, and, in any case, it should not exceed one month. The employer must take all necessary security measures, including sharing of data with authorized personnel only, pseudonymization/coding or encryption.

206 Article 205 of Law 4820/2021.

207 Joint Ministerial Decision (JMD) Δ1α/Γ.Π.οικ. 64232/15.10.2021.

208 European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences.

209 Coronavirus: a common approach for safe and efficient mobile tracing apps across the EU (13 May 2020); Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01; Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymized mobility data.

210 Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States, Version 1.0, 15.04.2020.

211 Protect human rights and public health in fighting COVID-19 (08 April 2020).

212 Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak; Twenty-first plenary session of the European Data Protection Board - Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic; Statement on the processing of personal data in the context of the COVID-19 outbreak. Adopted on 19 March 2020.

213 TechDispatch #1/2020: Contact Tracing with Mobile Applications.

Global Privacy and Security Law - Gilbert, § GRC.23, Greece,HEALTH INFORMATION

Francoise Gilbert, Global Privacy and Security Law § GRC.23 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

Apart from the GDPR provisions, which apply horizontally to all sectors, for health information the applicable rules also include the Medical Ethics Code, [214] 2071/1992 on the National Health System [215] and Article 371 of the Greek Penal Code, [216] according to which medical professionals must maintain their patients' medical data confidential and patients have the right of access to their health data.

In a number of its decisions, the Hellenic Data Protection Authority has placed significant emphasis on the organizational and technical measures that a data controller needs to implement, especially when sensitive health data are being collected and processed (without, however, referring to specific technologies and measures). [217]

Footnotes

214 Law 3418/2005 Art. 13 (medical confidentiality); Art. 14 (medical records).

215 Law 2071/1992 Art. 47 (rights of hospital patients).

216 Penal Code Art. 371 (breach of professional confidentiality).

217 Indicatively, Decisions 33/2007 (against the Ministry of Justice) and 43/2011 (against a public hospital).

Global Privacy and Security Law - Gilbert, § GRC.24, Greece,BIOMETRIC INFORMATION

Francoise Gilbert, Global Privacy and Security Law § GRC.24 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

The general principle, as formulated by the relevant decisions of the Hellenic Data Protection Authority, is that the use of biometric systems can be permitted in order to meet high security requirements for access control (identification and authentication) to specific physical areas (e.g., critical infrastructures [218]) or to computer systems (e.g., critical military or banking applications [219]), provided that this is always conducted in compliance with the principle of proportionality. [220]

See also the section on the protection of Employee Information for the special rules that apply in the case of the use of biometric information in the employment context.

Footnotes

218 Decision 9/2003 of the Hellenic Data Protection Authority on the use of the shape of the hand to control employees' access to high-risk facilities of the Athens Metro, the rapid-transit system in Athens); Decision 39/2004 and Decision 31/2010 of the Hellenic Data Protection Authority on the use of biometric systems at the Athens International Airport and the Thessaloniki Airport.

219 Decision 52/2008 of the Hellenic Data Protection Authority.

220 According to Art. 25(1) of the Constitution of Greece:

" *The rights of the human being as an individual and as a member of the society (…) are guaranteed by the State. (…) Restrictions of any kind which, according to the Constitution, may be imposed upon these rights (…) should respect the principle of proportionality.* " Also, according to Art. 52 of the EU Charter of Fundamental Rights, " *Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.* "

Global Privacy and Security Law - Gilbert, § GRC.25, Greece,SENSORS, VIDEO RECORDING

Francoise Gilbert, Global Privacy and Security Law § GRC.25 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

[A] Aerial Transportation; Drones

[1] Regulation—General Framework for Flights of Unmanned Aircraft Systems—UAS

Operation of Unmanned Aircraft Systems (UAS), free or tethered in ATHINAI FIR/HELLAS UIR is regulated by "Regulation—General framework for flights of Unmanned Aircraft Systems—UAS" [221] published in 2016 by

the Hellenic Civil Aviation Authority (HCAA), a civil service under the Ministry for Infrastructure and Transport. According to Art. 15 of the said Regulation, where during UAS flights (aerial work or other uses) personal data are being processed, this must be in accordance with applicable data protection legislation. The fines and sanctions provided by the GDPR and Law 4624/2019 apply. When HCAA is being notified about data protection issues relevant to the use of UAS, it must refer the issue to the Hellenic Data Protection Authority.

[2] Presidential Decree 98/2019

Greek Presidential Decree 98/2019 has introduced the rules for the deployment of drones for law enforcement purposes, an activity which was not permitted under Greek law until then. The scope of the said Presidential Decree is broad enough to allow police drones for the facilitation of air support to policing, surveillance and transmission of information to ground police forces.

Presidential Decree 98/2019 does not specifically regulate processing of collected data, for example regarding the retention period, or possible need for consultation with the Hellenic Data Protection Authority or performance of a data protection impact assessment, as per Articles 27-28 of the Law Enforcement Directive 2016/680.

Nonetheless, the Working Party 29 maintained that the use of drones operated by the police and other law enforcement authorities creates high risks for the rights and freedoms of individuals and directly interferes with the fundamental rights of respect for private life and protection of personal data. [222] Therefore, limitations to the exercise of these rights and freedoms must be provided for by law, only if and to the extent necessary in order to serve public interest in a democratic society or in order to protect the rights and freedoms of others. Moreover, the Presidential Decree 98/2019 does not specify which criminal activities establish the necessity for the deployment of law enforcement drones, thus leading to a blanket use, for any kind of policing and border management activities, theoretically allowing drone operations even for petty theft crimes without any prior authorization.

The potential increase of surveillance in public places, under certain circumstances, could lead to violation of fundamental human rights, such as privacy, data protection, or broadly, the freedom of expression. The omnipresence of police drones, collecting unspecified categories of personal data for statutorily undetermined law enforcement purposes, cultivates a chilling effect to individuals, and may eventually lead to mass surveillance mechanisms, which the CJEU has deemed in contradiction to the fundamental human rights. [223]

[3] Law 4961/2022

Articles 43–46 of Law 4961/2022 updated the legal framework for the use of Unmanned Aircraft Systems (UASs) for the provision of postal services. The Hellenic Telecommunications and Post Commission (EETT) authorizes, by decision, the use of UASs for the provision of postal services for which a general or specific authorization has already been authorized. Moreover, the EETT monitors the use of radio frequencies for the provision of postal services by UASs.

By decision of the competent Minister of Digital Governance upon the recommendation of the EETT and the Civil Aviation Authority (CAA), the specific technical characteristics and the technical security specifications of the UASs used for the provision of postal services, as well as any other relevant issue, will be defined.

Footnotes

221 Published in Government Gazette B/3152/30.09.2016; EN version, *available at* https://dagr.hcaa.gr/docs/HCAA%20UAS%20Regulation.pdf.

222 Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones.

223 Judgment of the Court (Grand Chamber), 8 April 2014, Digital Rights Ireland Ltd, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238; Judgment of the Court (Grand Chamber) of 21 December 2016, Tele2/Watson, Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970.

Global Privacy and Security Law - Gilbert, § GRC.26, Greece,DATA LOCATION REQUIREMENTS

Francoise Gilbert, Global Privacy and Security Law § GRC.26 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

There is typically an obligation for telecoms providers to carry out in-country data retention of traffic data and location data and the related data necessary to identify the user (Law 3917/2011 implementing Data Retention Directive 2006/24/EC). [224] However, in the light of the CJEU judgment invalidating the EU Data Retention Directive 2006/24/EC (Joined Cases C-293/12 and C-594/12), [225] and also considering recent CJEU judgments, delivered on October 6, 2020 (Cases C-623/17, C-511/18, C-512/18, C-520/18), [226] the validity and enforceability of the Law 3917/2011 is questionable although it is still technically in force.

A legislative committee had been set up, with the participation of the Hellenic Data Protection Authority to examine (*inter alia*) new provisions (amending or abolishing Law 3917/2011) in order to clarify this issue. [227] It is noted that in 2010 the Hellenic Data Protection Authority participated in the legislative committee for Law 3917/2011 and at that time the Greek Authority expressed the (minority) view that the data localization requirement in question is in breach of EU legislation.

Law 3917/2011 imposes data retention obligations for the purposes of the investigation, detection, and prosecution of serious crimes (a restrictive list of which is contained in Law 5002/2022). Law 3917/2011 applies to " *providers of publicly available electronic communications services or of public communications networks* "; retained data must be stored " *in physical media which are located exclusively in Greece* ."

Data retention period is 12 months starting from the date of the communication. It is noted that retained data do not include content of communication. The retention requirement covers traffic and location data of electronic communications services (non-content), i.e.:

- Data necessary to trace and identify the source of a communication;
- Data necessary to identify the destination of a communication;
- Data necessary to identify the date, time, and duration of a communication;
- Data necessary to identify the type of communication;
- Data necessary to identify users' communication equipment or what purports to be their equipment; and
- Data necessary to identify the location of mobile communication equipment (e.g., IP addresses of sender and receiver, log in/out times to the internet, names of subscribers).

Footnotes

224 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

225 Joined Cases C-293/12 and 594/12 Digital Rights Ireland Ltd v. Minister for Communication et al. and Kärtner Landesregierung et al. (CJEU, 8 April 2014), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293.

226 The Court of Justice confirms that EU law precludes national legislation requiring a provider of electronic communications services to carry out the general and indiscriminate transmission or retention of traffic data and location data for the purpose of combating crime in general or of safeguarding national security, https://curia.europa.eu/jcms/ upload/docs/application/pdf/2020-10/cp200123en.pdf.

227 Works of the said legislative committee seem to have ceased (without any deliverables).

Global Privacy and Security Law - Gilbert, § GRC.27, Greece,GOVERNMENT ACCESS TO PERSONAL DATA

Francoise Gilbert, Global Privacy and Security Law § GRC.27 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

[A] Limitations to Government Surveillance Activities

The Constitution of Greece [228] establishes the " *absolute inviolability*" of secrecy of communications, which can be side-stepped only for very specific cases (national security and very limited number of felonies, including *inter alia* child pornography, forgery, bribery, murder, robbery, terrorist acts, computer fraud, extortion, etc.) and only under the guarantees and supervision of the judiciary and the involvement of a constitutionally established independent authority (with the sole purpose of safeguarding the confidentiality and secrecy of communications).

A list of the felonies for which " *lifting of secrecy of communications* " can be allowed and the procedures, time limits, and technical and organizational safeguards that need to be followed are included in Law 5002/2022, which annulled Law 2225/1994, and in Presidential Decree 47/2005. Applicable is also Article 254 of the Criminal Procedure Code (investigative actions against organized crime). Only the competent Public Prosecutor or a Judicial Authority or other political, military or police public authority, competent for an issue of national security requiring the " *lifting of secrecy* ," may submit a request for " *lifting of secrecy* ," which then can be ordered by the Public Prosecutor of the Greek Court of Appeals or the competent Judicial Council (exceptionally by the Public Prosecutor of the Greek First Instance Court).

The " *lifting of secrecy* " applies to communication conducted via communication networks or via communication service providers. The types and forms of communication which are subject to the " *lifting of secrecy* " are (*inter alia*) telephone (fixed and mobile), data communication via data networks, internet communication, wireless communication, satellite communication, and services provided in the framework of the above types/forms (e.g., automatic answering machine, SMS/MMS, access to websites, access to databases, e-mail, electronic transactions, directory information, emergency services).

The issue of the "lifting of secrecy of communications" (which data it covers, which authorities can order it and what procedure must be followed) has been discussed and debated in Greece for many decades. Indicative of the legal uncertainty over this issue are the different approaches adopted by the Independent Authorities on the one hand (the Hellenic Data Protection Authority and the Hellenic Authority for Communication Security and Privacy—constitutionally consolidated independent authorities) and by the Public Prosecutors of the Supreme Court on the other hand, interpreting and enforcing the same legal provisions.

[B] Video Surveillance in Public Places

Presidential Decree 75/2020 (the "PD"), issued on September 4, 2020, regulates the use of surveillance systems in public places. Notably, a draft version of the PD had been reviewed by the Hellenic Data Protection Authority, which issued its Opinion 03/2020 with specific comments and guidance; most of the DPA's comments have been taken into account in the final and currently applicable version of the PD.

Within the scope of the PD fall all types of surveillance systems that process personal data, regardless of their specifications and the technology used.

Permitted processing purposes restrictively include (a) the prevention and suppression of certain criminal acts [229] (identification of perpetrators and collection of evidence) and (b) traffic management (dealing with emergencies on the road network, traffic control and prevention and management of road accidents). The Hellenic Police is controller for both processing purposes, whereas the Hellenic Coastguard and the Hellenic Fire Service are controllers for the purpose of prevention and suppression of certain criminal acts. When a different public authority operates the surveillance system, said public authority will act under the capacity of joint controller.

The PD sets the legal and technical principles and conditions for the establishment and the functioning of surveillance systems; for instance, the system can be used only when objectives cannot be achieved equally as effectively as with other less privacy intrusive means (principle of proportionality), sufficient evidence must exist that criminal activity is taking place or will take place (the controller must reasonably believe that, in certain public spaces, public security is under significant risk), etc. Special provisions and conditions apply for the use of portable surveillance devices, [230] also for the use of zooming functionality (which is possible only upon reasoned decision of the controller and subsequent approval by the Public Prosecutor). The use of surveillance systems in outdoor public gatherings can be permitted only on the basis of reasoned decision of the controller and approval by the Public Prosecutor; the organizer of the gathering and participants must be informed accordingly (further conditions apply).

According to the PD, image processing for the needs of traffic management must be limited to identification of license plates and vehicle type (passenger cars, trucks, buses, etc.). Processing of sound (to the extent that this can lead to identification of persons) can be permitted only, as a matter of exception, upon reasoned decision of the controller, which must have been further approved by the Public Prosecutor and only for the specific criminal acts provided by Law 5002/2022 (regulating “lifting of secrecy of communications”). [231]

Data can be retained for a maximum 15 days period as of collection, unless further retention is required for the needs of crime investigation; specifically, data collected during public outdoor gatherings must be deleted within 48 hours as of the end of the gathering (unless, again, further retention is required for the needs of crime investigation). Moreover, in cases of reasonable suspicion that a data subject is preparing criminal activities or will likely commit criminal acts in the future, data can be retained for an indefinite period, which must be re-assessed every two years.

Further rules apply for data recipients and data subject rights and technical and organizational security measures.

Footnotes

228 Greek Constitution, Article 19 (Secrecy of Correspondence).

229 According to Law 3917/2011, Art. 14, par. 1.

230 The Hellenic Data Protection Authority had criticized the lack of independent or judicial oversight on the use of portable surveillance devices; however, relevant provision has not been included in the PD.

231 Notably, the Hellenic Data Protection Authority raised concerns regarding the compliance of the said provision with the Greek Constitution, the applicable legal framework regulating “lifting of secrecy of communications” (Law 5002/2022 and Presidential Decree 47/2005) and the Code of Criminal Procedure (special investigative techniques).

Global Privacy and Security Law - Gilbert, § GRC.28, Greece,IMPLEMENTATION OF THE LAW ENFORCEMENT DIRECTIVE (EU) 2017/680

Francoise Gilbert, Global Privacy and Security Law § GRC.28 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

Chapter D of Law 4624/2019 has transposed Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

The Hellenic Data Protection Authority has strongly criticized transposition of Directive (EU) 2016/680; [232] as argued by the Authority, in many cases, certain provisions of the Directive have not been transposed, in other cases, the text of the Directive has been transposed "as is" without any adaptation to national legislation, while, in certain cases, transposition is incorrect.

Law 4624/2019 sets the scope of application, [233] mentioning that provisions of Chapter D shall apply to the processing of personal data by "public authorities" competent for the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. [234]

Chapter D of Law 4624/2019 has transposed definitions included in the Directive (EU) 2016/680. [235] However, as pointed out by the Hellenic Data Protection Authority, [236] Chapter D has failed to include a definition of "competent (public) authority." [237] Moreover, while a definition of "supervisory authority" is typically included in Chapter D, such definition has not been properly transposed as no reference is being made to a specific competent national authority, namely the Hellenic Data Protection Authority.

Law 4624/2019 [238] refers to the principles that competent public authorities must follow when processing personal data within the scope of Chapter D; these include the principles of lawfulness, fairness, purpose limitation, proportionality, accuracy, storage limitation, data minimization, security.

Chapter D of Law 4624/2019 regulates processing for a purpose, within or outside the scope of Chapter D, other than that for which the personal data are collected and sets the requirement for such processing. [239] However, as highlighted by the Hellenic Data Protection Authority, [240] further processing for a purpose outside the scope of Chapter D [and essentially outside the scope of Directive (EU) 2016/680], other than that for which the personal data were originally collected, is inconsistent with Art. 4(2) of Directive (EU) 2016/680. [241]

Chapter D of Law 4624/2019 also regulates processing for archiving in the public interest, scientific, statistical or historical use, subject to appropriate safeguards for the rights and freedoms of data subjects, which may include anonymization, data separation, etc. [242]

Rules on automated individual decision-making have been transposed in Chapter D of Law 4624/2019; [243] however, according to the Hellenic Data Protection Authority, said rules have been inadequately implemented failing to introduce specific "appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller." [244]

Moreover, Chapter D of Law 4624/2019 has implemented and introduced provisions on the rights of the data subject, [245] including right of access; [246] right to rectification or erasure of personal data and restriction of processing; right to lodge a complaint with the supervisory authority; and rights of the data subject in criminal investigations and proceedings.

Chapter D of Law 4624/2019 has introduced certain obligations for controllers and processors, [247] covering, *inter alia*, security of processing, notifications of data breach to supervisory authority and data subjects, data protection impact assessment, prior consultation of the supervisory authority, [248] records of processing activities, data protection by design and by default, time-limits for storage, [249] logging.

Furthermore, the controller and the processor shall keep logs in automated processing systems for at least the following processing operations: collection, alteration, consultation, disclosure (including transfers), combination and erasure. [250] The logs shall be used solely for the following purposes: for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings. According to Law 4624/2019 Art. 74(4), the said logs must be deleted at the end of the year following the year during which such logs have been created. The Hellenic Data Protection Authority has criticized Art. 74(4), highlighting that failure to expressly permit retention until the end of the above-mentioned operations could lead to unacceptable results; for instance, if an investigation is being carried out by the supervisory authority or in the course of a criminal proceeding, an obligation to delete relevant logs has been introduced regardless of the completion of the relevant operation. [251]

Chapter D of Law 4624/2019 has also implemented and introduced provisions on transfers of personal data to third countries or international organizations, [252] cooperation between supervisory authorities. [253]

Sanctions for breach of the provisions of Chapter D of Law 4624/19 [254] include civil liability, criminal sanctions [255] and administrative sanctions. [256]

The adoption of Law 5002/2022 brought certain changes to Law 4624/2019, insofar the transposition of Directive 2016/680. To be specific, Article 45A was introduced in Law 4624/2019, stipulating that the processing of personal data shall be lawful only if based on national or Union legislation and necessary for the performance of a task carried out by the competent authorities for the purposes referred to in Article 43.

Another interesting addition is new Article 84A of Law 4624/2019, which provides for the disclosure of personal data by the Public Prosecutor. By order of the competent Prosecutor, the Hellenic Police shall make public, for a period not exceeding six (6) months, the identity, image and criminal record of a person accused or convicted of felonies or specific misdemeanors, including inter alia crimes against sexual freedom and economic exploitation of sexual life.

Footnotes

232 Hellenic Data Protection Authority, Opinion 1/2020, p. 21.

233 Law 4624/2019 Art. 43 [transposing Directive (EU) 2016/680 Art. 1 and Art. 2].

234 As argued by the Hellenic Data Protection Authority (Opinion 1/2020, p. 21-22), Directive (EU) 2016/680 Art. 1(2)(a) and (partly) Art. 1(1) have not been transposed; as a result, Greek implementation does not clearly transpose the objective of the Directive, which is the protection of data during processing for the purposes of crime prosecution.

235 “Personal data,” “processing,” “restriction of processing,” “profiling,” “pseudonymisation,” “filing system,” “controller,” “processor,” “recipient,” personal data breach,” “genetic data,” “biometric data,” “data concerning health,” “supervisory authority,” “international organisation”; also includes definitions for “special categories of personal data” and “consent.”

236 Hellenic Data Protection Authority, Opinion 1/2020, p. 22.

237 Directive (EU) 2016/680 Art. 3(7)(a).

238 Law 4624/2019 Art. 45 [transposing Directive (EU) 2016/680 Art. 4].

239 Law 4624/2019 Art. 47 [transposing Directive (EU) 2016/680 Art. 4(2)].

240 Hellenic Data Protection Authority, Opinion 1/2020, p. 22.

241 *See also* Directive (EU) 2016/680 Preamble § 29.

242 Law 4624/2019 Art. 48 [transposing Directive (EU) 2016/680 Art. 4].

243 Law 4624/2019 Art. 52 [transposing Directive (EU) 2016/680 Art. 11].

244 Hellenic Data Protection Authority, Opinion 1/2020, p. 23.

245 Law 4624/2019 Art. 53-59 [transposing Directive (EU) 2016/680 Art. 12-18].

246 The Hellenic Data Protection Authority has pointed out that the option of the data subjects to exercise their right through the competent supervisory authority [per Directive (EU) 2016/680 Arts. 15 and 17] has been inadequately transposed as a right to lodge a complaint with the supervisory authority (Opinion 1/2020, p. 23).

247 Law 4624/2019 Art. 60-74 [transposing Directive (EU) 2016/680 Arts. 5-7, 9, 19-31].

248 The Hellenic Data Protection Authority has pointed out that certain content of this regulation [Law 4624/2019 Art. 60(6)] is not provided by the Directive (EU) 2016/680 (Opinion 1/2020, p. 23).

249 The Hellenic Data Protection Authority has pointed out that, while relevant Art. 73(4) refers to erasure of personal data or to periodic review of the need for the storage of personal data and to the procedural measures that should ensure that those time limits are observed, it fails to introduce specific criteria, per Directive (EU) 2016/680 Preamble § 33 (Opinion 1/2020, p. 24).

250 Law 4624/2019 Art. 73 [transposing Directive (EU) 2016/680 Art. 25]

251 Hellenic Data Protection Authority, Opinion 1/2020, p. 24.

252 Law 4624/2019 Art. 75-78 [transposing Directive (EU) 2016/680 Arts. 35, 37-39]; relevant are also the EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, *available at* https://edpb.europa.eu/sites/default/files/files/file1/recommendations012021onart.36led.pdf_en.pdf.

253 Law 4624/2019 Art. 79 [transposing Directive (EU) 2016/680 Art. 50].

254 Law 4624/2019 Art. 80-82 [transposing Directive (EU) 2016/680 Arts. 54, 56, 57].

255 Applicable are criminal sanction provided by Law 4624/2019 Art. 38. CRC. 17[B][3].

256 Administrative sanctions may be up to EUR 2.000.000.

Global Privacy and Security Law - Gilbert, § GRC.29, Greece,IMPLEMENTATION OF THE NIS AND NIS2 DIRECTIVES

Francoise Gilbert, Global Privacy and Security Law § GRC.29 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

[A] NIS Directive (EU) 2016/1148

Law 4577/2018 has transposed the NIS Directive (EU) 2016/1148 [257] in the Greek legal system. Law 4577/2018 has introduced measures with a view to achieving a high level of security of network and information systems and applies to Operators of Essential Services (OESs) and to Digital Service Providers (DSPs). OESs include entities in the energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution, and digital infrastructure sectors. DSPs include online marketplaces, online search engines, and cloud computing services.

The General Secretariat for Digital Policy of the Ministry of Digital Policy, Telecommunications and Media has been designated as the National Cyber Security Authority, which is competent to monitor applications of Law 4577/2018, to operate as national single point of contact on the security of network and information systems to consult and cooperate with other EU and Greek Authorities and Regulators. The Cyberdefense Directorate of the Hellenic National Defense General Staff has been designated as the Computer Security Incident Response Team (CSIRT) responsible for risk and incident handling in Greece.

Law 4577/2018 establishes security and notification requirements for OESs and DSPs. OESs must notify, without undue delay, the National Cyber Security Authority (General Secretariat for Digital Policy—Ministry of Digital Policy, Telecommunications, and Media) and the Computer Security Incident Response Team (CSIRT)

of incidents having a significant impact on the continuity of the essential services they provide. DSPs must notify the National Cyber Security Authority and the CSIRT without undue delay of any incident having a substantial impact on the provision of a service that they offer within the Union.

It is noted that data breach notifications introduced by other legislation (e.g., the GDPR) remain unaffected.

Sanctions for breach of Law 4577/2018 (no notification/delay of notification, failure to take appropriate organizational/technical measures, non-provision or unjustified delay in the provision of information, if requested by the National Cybersecurity Authority) include administrative fines imposed by the Minister of Digital Policy, Telecommunications and Information (following proposal by the National Cybersecurity Authority), which range from EUR 15.000 to EUR 200.000 depending on gravity and repetitiveness.

[B] NIS2 Directive (EU) 2022/2555 Repealing NIS Directive

The Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) was published in the Official Gazette of the European Union on December 27, 2022, and became effective as of January 16, 2023. Pursuant to Article 41 of the NIS 2 Directive, by October 17, 2024, Member States must transpose the NIS2 Directive into their national legislation, and the transposition laws shall apply from October 18, 2024. On the same date, the NIS Directive will be repealed.

Footnotes

257 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Global Privacy and Security Law - Gilbert, § GRC.30, Greece,DIGITAL GOVERNANCE

Francoise Gilbert, Global Privacy and Security Law § GRC.30 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

Newly introduced Law 4727/2020, regulating digital governance (also transposing Directive (EU) 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies and Directive (EU) 2019/1024 on open data and the re-use of public sector information), includes certain provision with regard to data protection.

[A] General Principles of Digital Governance

Public sector entities which provide digital public services must respect the protection of personal data and the privacy of individuals. The said entities are obliged to take by design appropriate technical and organizational measures for the protection of personal data, also during configuration, procurement and operation of the information technology systems and digital services, ensuring by default compliance with the data minimization and purpose principles.

[B] Automated Provision of Digital Public Services

GDPR and Law 4624/2019 rules apply to data transfers between public sector bodies, also to the interconnection of electronic files or databases maintained by public-sector bodies and generally to fully automated processing with the support of information technology systems and databases, for the needs of

provision of digital public services, also in order for public sector bodies to respond to applications and inquiries made by individuals and legal entities.

[C] Personal Number

Law 4727/2020 introduces the "Personal Number," a unique number assigned to each individual and used for mandatory verification of his/her identity in transactions with public sector bodies. The General Secretariat of Information Systems for Public Administration is responsible for the provision of the said identity verification services, also responsible to ensure interoperability of the information technology systems used by competent public sector bodies, taking into account applicable data protection legal framework.

[D] Open Data

Law 4727/2020 transposes Directive (EU) 2019/1024 on open data and the re-use of public sector information. Notably, relevant rules do not apply to documents to which access is either excluded or restricted for reasons of protection of personal data, or access is permitted, but re-use is contrary to data protection legislation or provisions protecting private life and the integrity of the individual.

[E] Digital Transparency

Law 4727/2020 has introduced the obligation for certain public sector bodies to publish online laws, presidential decrees and acts issued by the said bodies. In this context, publishing and search options of this information must take into account applicable data protection legislation, state secrets, intellectual and industrial property laws, and statutory confidentiality obligations; acts that include special categories of personal data and personal data related to criminal convictions and offenses must not be published.

[F] Infrastructures

Public Sector Government Clouds (G-Cloud), Research and Education Sector Clouds (RE-Cloud) and Health Sector Clouds (H-Cloud) can be interconnected, aiming at optimal provision of digital public services and creation of systems for backup, business continuity, and disaster recovery, always in compliance with applicable data protection legislation (certain exceptions apply).

Global Privacy and Security Law - Gilbert, § GRC.31, Greece,WHISTLEBLOWER PROTECTION DIRECTIVE

Francoise Gilbert, Global Privacy and Security Law § GRC.31 (First Edition, Supp. #42 2009)
First Edition, Supp. #42

Last Update: 1/2024

[A] Overview of the Directive

Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the Protection of Persons who Report Breaches of Union law ("Whistleblower Protection Directive") was adopted on October 23, 2019, and entered into force on December 16, 2019. [258] The Whistleblower Protection Directive establishes rules and procedures to protect "whistleblowers," i.e., individuals who report certain breaches of EU laws that have come to their attention in a work-related context.

[B] Implementation in Greece

Law 4990/2022 (the “Whistleblowing Law”) transposed the Whistleblower Protection Directive into Greek legislation in November 2022.

[1] Reporting Protected Under the Whistleblowing Law

Whistleblower protection refers to the reporting of wrongdoing related to EU law, in particular (i) infringements with regard to public procurement, financial services, products and markets, prevention of money laundering and terrorist financing, product safety and compliance, transport safety, protection of the environment, radiation protection and nuclear safety, food and feed safety, animal health and welfare, public health, consumer protection, as well as protection of privacy and personal data, and security of network and information systems; (ii) infringements affecting the EU economic interests; and (iii) infringements related to the EU internal market.

[2] Protection Granted to Whistleblowers

Pursuant to the Whistleblowing Law, any form of retaliation against whistleblowers shall be prohibited, including threats and acts of retaliation, while whistleblowers shall not be able to be held liable. In the event of retaliation, whistleblowers shall be entitled to full compensation for the damages suffered, while any acts of retaliation, including dismissal, shall be invalid. Whistleblowers are also entitled to free legal advice and representation, as well as free psychological support.

[3] Whistleblowers Protected

The personal scope of the Whistleblowing Law is broad, since, not only current or former employees, but also job applicants, self-employed persons, consultants, home workers, shareholders and persons belonging in the administrative, management or supervisory bodies of the company, including non-executive members, volunteers, paid or unpaid trainees, as well as any person working under the supervision and direction of contractors, subcontractors and suppliers of a company are eligible as whistleblowers.

[4] Internal Reporting Channels

The Whistleblowing Law establishes a framework for reporting violations of EU law at two levels. At the first level, whistleblowers shall report such violations internally, to the person within the organization designated for this purpose. In this context, the Whistleblowing Law requires that public and private entities with at least 50 employees or, regardless of the number of employees, private companies operating in financial services, products and markets, as well as transport and environment sectors, establish internal reporting procedures regarding violations of EU that shall be operated by a person (employee or third party) designated for this purpose, whose responsibilities are laid down in the Whistleblowing Law.

[5] External Reporting Channels

As a second level, the Whistleblowing Law establishes the National Transparency Authority as the single external reporting channel in Greece, allowing whistleblowers either to resubmit the report they have already submitted to an internal channel to the external reporting channel or to submit the report directly to the external reporting channel.

[6] Sanctions and Administrative Fines

The Whistleblowing Law provides for both criminal sanctions and monetary fines for persons who (i) prevent or attempt to prevent reporting; (ii) retaliate or take malicious action against whistleblowers; or (iii) infringe their obligation to respect the confidentiality of the identity of the whistleblowers. In addition, the Law provides for both criminal sanctions and monetary fines for persons who knowingly report or publicly disclose false information.

Lastly, the Law provides for administrative fines from EUR 10,000 to EUR 500,000 in case of any infringements thereof has taken place for the benefit or on behalf of a legal person.

[7] Anonymity of Whistleblowers

The Whistleblowing Law requires that personal data and any kind of information leading, directly or indirectly, to the identification of the whistleblowers shall not be disclosed to anyone other than the designated persons responsible for receiving or monitoring the reports, unless the whistleblower consents thereto. To this end, the above-mentioned entities shall take appropriate technical and organizational measures, such as pseudonymization techniques, when monitoring the report and communicating with the competent authorities. Exceptionally, the identity of the whistleblower and any other information may be disclosed only where required by EU or national law, in the context of investigations by competent authorities or in the context of judicial proceedings, and where this is necessary to serve the purposes of the Whistleblowing Law or to safeguard the legitimate rights of the whistleblower.

Finally, it shall be noted that the Whistleblowing Law provides the same level of protection to anonymous whistleblowers in case they are identified at a later stage, leaving room for anonymous reporting.

Footnotes

258 Text *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX: 32019L1937.