Data Protection in Greece: Overview

by Popi Papantoniou and Valeria Kokkinou, Bahas, Gramatidis & Partners LLP, with Practical Law Data Privacy Advisor

Country Q&A | Law stated as of 15-Jun-2021 | Greece

A Q&A guide to data protection in Greece.

This Q&A guide gives a high-level overview of the data protection laws, regulations, and principles in Greece, including the main obligations and processing requirements for data controllers, data processors, or other third parties. It also covers data subject rights, the supervisory authority's enforcement powers, and potential sanctions and remedies. It briefly covers rules applicable to cookies and spam.

To compare answers across multiple jurisdictions, visit the Data Protection Country Q&A Tool.

Regulation

Legislation

1. What national laws regulate the collection, use, and disclosure of personal data?

Data Protection Law

The European Union (EU) General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) governs data protection and applies directly in each EU member state, including Greece. The GDPR replaced the EU Data Protection Directive (95/46/EC) (Data Protection Directive) and the prior Greek data protection law, introducing a single legal framework across the EU. However, several GDPR provisions allow EU member states to enact national legislation specifying, restricting, or expanding the scope of some requirements.

Greece enacted Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law), which supplements the GDPR and changes some of its requirements. The Hellenic Data Protection Authority (HDPA) has also issued:

- Opinion 1/2020 (in Greek) to clarify the Data Protection Law's compatibility with the GDPR.
- Several directives, decisions, and opinions on personal data protection and processing under the Data Protection Directive and the prior Law 2472/1997 on the Protection of Individuals Regarding Processing

Personal Data, which contains certain provisions that remain in effect (Article 84, Data Protection Law; see HDPA: Acts of the Authority (in Greek)). According to the HDPA, this guidance remains in force and applies in parallel with the GDPR and the Data Protection Law.

For additional GDPR guidance from the HDPA, *see* GDPR Data Protection Authority Guidance Tracker by Country (EEA): Greece. This Q&A discusses key derogations and requirements under the Data Protection Law.

Greece also:

- Signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) (Convention 108) on February 17, 1983 and August 11, 1995 respectively. Convention 108 was effective December 1, 1995.
- Signed the Additional Protocol to Convention 108 on supervisory authorities and transborder data flows (ETS No. 181) on November 8, 2001.
- Signed the Protocol amending Convention 108 (CETS No. 223) on September 6, 2019.

(See Council of Europe: Treaty List for Greece.)

For more on Greece's implementation of the GDPR, see Practice Note, Greek Implementation of the GDPR.

Other Relevant Laws

Several other Greek laws apply to personal data collection, use, and disclosure, for example:

- Law 4579/2018 on the Obligations of Air Carriers in Relation to Passenger Name Records Data (in Greek), which transposes the EU Passenger Name Record Directive (Directive (EU) 2016/681) on the use of passenger name record (PNR) data for the prevention, detection, investigation, and prosecution of terrorist offenses and serious crime.
- Law 3471/2006 on the Protection of Personal Data and Privacy in the Electronic Telecommunications Sector, as amended (in Greek), which implements the EU E-Privacy Directive (Directive 2002/58/EC), as amended by the EU Citizens' Rights Directive (Directive 2009/136/EC).
- Legislative Decree 1059/1971, as amended, which regulates bank secrecy.
- Article 40 of Law 3259/2004, as amended, which regulates retention of data related to economic behavior.
- Law 4557/2018 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, as amended, which implements Directive (EU) 2015/849, in combination with Law 3932/2011 on the Establishment of an Anti-Money Laundering Authority.

The details of these other laws are outside the scope of this Q&A, which focuses on the GDPR and the Data Protection Law. For more on other relevant EU laws that apply in Greece but are beyond the scope of this Q&A, see Country Q&A, Data Protection in the EU: Overview: Other Relevant Laws.

Scope of Legislation

2. To whom do the laws apply?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1). Both the GDPR and Greece's Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) apply to:

- Controllers**.** A controller, formerly known as a data controller, is any natural or legal person, public authority, agency, or any other body that determines the purposes and the means of the data processing alone or jointly with others (Article 4(7), GDPR).
- Processors**.** A processor, formerly known as a data processor, is any natural or legal person, public authority, agency, or any other body that processes personal data on the controller's behalf (Article 4(8), GDPR).
- Data subjects**.** Data subjects are individuals to whom personal data relates (Article 4(1), GDPR; for more on what constitutes personal data, see Question 3).

The Data Protection Law does not separately define any of the GDPR definitions set out above.

3. What personal data does the law regulate?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1). Both the GDPR and Greece's Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) regulate personal data processing (Articles 2(1) and 4(2), GDPR; Articles 1 and 2, Data Protection Law).

The GDPR:

- Defines personal data as information relating to an identified or identifiable natural person, called a data subject. An identifiable natural person is one who can be identified, directly or indirectly, by reference to identifiers such as the person's:
    - name, address, and telephone number;
    - job title;
    - date of birth;
    - location data;

- online identifiers like IP addresses, cookies, and radio frequency identification tags (see Recital 30, GDPR); or
- physical, physiological, genetic, mental, economic, cultural, or social identity.

(Article 4(1), GDPR.)

- Imposes additional limitations on and requires more rigorous protection for special categories of personal data, previously known as sensitive personal data (Article 9(1), GDPR).
- Defines genetic data, biometric data, and health data (Article 4(13) to (15), GDPR).
- Allows EU member states to enact national laws specifying, restricting, or expanding the requirements for processing special categories of personal data (Article 9(4), GDPR).

For more on processing special categories of personal data, see Question 11.

4. What acts are regulated?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1). Subject to certain exemptions, both the GDPR and Greece's Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) apply to personal data processing:

- Wholly or partly by automated means.
- Other than by automated means if the personal data forms or is intended to form part of a filing system.

(Articles 2(1) and (2), GDPR; Article 2, Data Protection Law.)

The Data Protection Law does not separately define processing, so the GDPR's definition applies. The GDPR defines processing as any operation or set of operations that is performed on personal data or sets of personal data, whether automated or not, such as:

- Collection.
- Recording.
- Organization.
- Structuring.
- Storage.
- Adaptation or alteration.

- Retrieval.
- Consultation.
- Use.
- Disclosure by transmission.
- Dissemination or otherwise making available.
- Alignment or combination.
- Restriction, erasure, or destruction.

(Article 4(2), GDPR.)

GDPR Articles 85 to 91 permit EU member states to enact further rules in seven specific processing situations. The Data Protection Law introduces further rules that apply to processing:

- For journalistic purposes or academic, artistic, or literary expression under GDPR Article 85 (Article 28, Data Protection Law).
- For archiving in the public interest, scientific or historical research or statistical purposes under GDPR Article 89 (Articles 29 and 30, Data Protection Law).
- In the employment context under GDPR Article 88 (Article 27, Data Protection Law).

The Data Protection Law does not expressly address the GDPR's other specific processing situations under Articles 86, 87, 90, or 91, though it includes a general reference to the Code of Administrative Procedure, which regulates access to public documents (Article 42, Data Protection Law). However, other Greek laws may apply. For more on the Data Protection Law's derogations for specific processing situations, see Practice note, Greek Implementation of the GDPR: Derogations for Specific Processing Situations and Processing in the Employment Context.

The rules applicable to processing under GDPR Articles 85, 88, and 89 may also affect data subject rights (see Question 12 and Question 13).

For more on:

- The jurisdictional scope of the GDPR and the Data Protection Law, see Question 5.
- The GDPR's and the Data Protection Law's exemptions, see Question 6.
- The GDPR's definitions, see Practice Note, Overview of EU General Data Protection Regulation: GDPR: definitions.

5. What is the jurisdictional scope of the rules?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1). For more on the GDPR's jurisdictional scope and when the requirement to designate a local representative in the European Union (EU) applies, see Country Q&A, Data Protection in the EU: Overview: Question 5.

Some EU member states have passed national laws that include a territorial scope provision that mirrors GDPR Article 3. Other member states' laws include different applicability language or do not include a territorial scope provision. The territorial scope provision in Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) states that it applies to controllers and processors:

- That process personal data in Greece.
- Established in Greece that process personal data in the context of that establishment.
- Not established in an EU member state, or the European Economic Area that fall within the GDPR's scope.

(Article 3, Data Protection Law.)

The Data Protection Law also applies to public bodies (Articles 2(a) and 3, Data Protection Law).

6. What are the main exemptions (if any)?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1). For more on the GDPR's main exemptions, see Country Q&A, Data Protection in the EU: Overview: Question 6.

Like the GDPR, Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) does not apply to personal data processing by private bodies during a purely personal or household activity (Article 2(b), Data Protection Law).

The following GDPR provisions also do not apply to the extent necessary to reconcile personal data protection rights with the right to freedom of expression and information, including processing for journalistic purposes or academic, artistic, or literary expression:

- Chapter II (principles), except for Article 5.
- Chapter III (rights of the data subject).
- Chapter IV (controller and processor), except for Articles 28, 29, and 32.

- Chapter V (transfer of personal data to third countries or international organizations).
- Chapter VII (cooperation and consistency).
- Chapter IX (specific data processing situations).

(Article 28(2), Data Protection Law.)

For more on how processing for journalistic purposes affects data subjects' rights and controllers' related obligations, see Question 12 and Question 13. For more on specific processing situations in Greece, see Practice note, Greek Implementation of the GDPR: Derogations for Specific Processing Situations.

Notification

7. Is notification or registration with a supervisory authority required before processing data?

For information on the Hellenic Data Protection Authority's (HDPA) notification, registration, or authorization requirements, see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: Greece: Questions 2 and 3. For the HDPA's contact information, see Regulator Details.

Main Data Protection Rules and Principles

Main Obligations and Processing Requirements

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1) and sets out the following six principles that govern personal data processing:

- **Lawful, fair, and** transparent **processing.** Controllers must process personal data lawfully, fairly, and in a transparent manner in relation to the data subject. The European Data Protection Board has endorsed Article 29 Working Party guidelines on transparency (see *European Commission: Guidelines on transparency under the GDPR (WP260) (April 11, 2018)*).
- Purpose limitation**.** Controllers:

    - may only collect personal data for specified, explicit, and legitimate purposes; and
    - may not further process personal data for an incompatible purpose except for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

- Data minimization**.** Controllers may only process personal data that is adequate, relevant, and limited to what is necessary for the purposes of their processing.
- **Accuracy.** Personal data must be accurate and up to date where necessary. Controllers must take every reasonable step to erase or rectify inaccurate date without delay.
- **Storage limitation.** Controllers generally may not store personal data in a form that permits identification of data subjects for longer than is necessary for the purposes of their processing. With appropriate technical and organizational measures to safeguard data subjects' rights and freedoms, there are again limited exceptions under GDPR Article 89(1), for:
    - archiving purposes in the public interest;
    - scientific or historical research purposes; or
    - statistical purposes.
- **Integrity and confidentiality.** Controllers must process personal data in a manner that ensures appropriate security, using appropriate technical and organizational measures to protect against:
    - unauthorized or unlawful processing;
    - accidental loss;
    - destruction; or
    - damage.

(Article 5(1), GDPR; see Question 15.)

For more on accountability and GDPR compliance, see Practice Note, Demonstrating Compliance with the GDPR: Accountability and Demonstrating Compliance.

In addition to complying with these six principles, controllers must also, among other things:

- Take appropriate measures to provide processing-related information to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language (Article 12, GDPR; see Question 12).
- Facilitate the exercise of data subjects' rights (see Question 13).
- Properly secure personal data (see Question 15).
- Record all personal data breaches and report relevant breaches to the relevant supervisory authority and data subjects in certain circumstances (Articles 33 and 34, GDPR; see Question 16).

- Meet certain obligations when engaging processors (see Question 17).
- Keep written or electronic records with specified information about their processing activities, depending on the number of their employees and the nature of the processing (Article 30, GDPR).
- Designate a European Union representative in certain circumstances (Articles 3(2) and 27(1), GDPR).
- Carry out an assessment of the impact of their processing operations when necessary (Article 35, GDPR).
- Consult the supervisory authority before processing if a data protection impact assessment under GDPR Article 35 indicates that the processing would result in a high risk if the controller fails to take measures to mitigate the risk (Article 36, GDPR).
- Designate a data protection officer (DPO) if:
    - a public authority or body carries out the processing, except for courts acting in their judicial capacity;
    - the controller's core activities are processing operations that require regular and systematic monitoring of data subjects on a large scale by virtue of their nature, scope, or purposes;
    - the controller's core activities are processing of special categories of data or personal data relating to criminal convictions and offenses on a large scale; or
    - an EU member state stipulates by national regulation that a DPO is required.

  (Article 37(1), GDPR.)
- Publish the DPO's contact details and communicate them to the supervisory authority (Article 37(7), GDPR).

Data Protection Officers

The GDPR allows EU member states to require DPO appointments in additional situations (Article 37(4), GDPR).

Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) imposes additional requirements for DPOs in public bodies (Articles 6 to 8, Data Protection Law).

For information on whether private-sector controllers operating in Greece are required to appoint a DPO, see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: Greece: Questions 4 and 5.

Purpose Limitation

The GDPR generally restricts data processing to the original collection purpose unless an exception applies, for example:

- The data subject consents to processing for a secondary purpose.
- An EU or EU member state law, which is a necessary and proportionate measure to safeguard certain important objectives, permits the processing for a secondary purpose.

(Article 6(4), GDPR.)

Without data subject consent, any secondary processing purpose must both:

- Remain compatible with the original processing purpose.
- Satisfy the conditions in GDPR Article 6(4).

To determine the secondary processing purpose's compatibility, the controller should consider the criteria specified in GDPR Article 6(4) (see Practice Note, Overview of EU General Data Protection Regulation: Further compatible processing).

The Data Protection Law allows:

- Public bodies to process personal data for secondary purposes when necessary to perform their tasks and provided the processing is necessary to:
    - verify information a data subject provides if there are reasonable grounds to believe that information is incorrect;
    - prevent risks to national security, defense, or public security;
    - secure tax and customs revenue;
    - prosecute criminal offenses;
    - prevent serious harm to another person's rights; or
    - produce official statistics.

    (Article 24(1), Data Protection Law.)
- Private bodies to process personal data for secondary purposes when necessary to:
    - prevent threats to national or public security at a public body's request;
    - prosecute criminal offenses; or
    - establish, exercise, or defend legal claims, unless the data subject's interests override the grounds for processing.

    (Article 25(1), Data Protection Law.)

However, according to HDPA Opinion 1/2020 (in Greek), Data Protection Law Articles 24 and 25 establish bases to process personal data for purposes other than initially collected. The HDPA takes the position that the GDPR does not authorize national law to establish new legal bases for processing other than those already provided in GDPR Article 6. The HDPA does not consider these provisions a necessary and proportionate measure to safeguard the objectives stated in GDPR Article 23. Therefore, according to the HDPA, Data Protection Law Articles 24 and 25 are not in line with the GDPR and the HDPA will not apply them.

Special rules apply to processing special categories of personal data for a secondary purpose (Articles 24(2) and 25(2), Data Protection Law; see Question 11).

9. Is the consent of data subjects required before processing personal data?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1) and sets out six lawful bases for processing personal data. One of those bases is obtaining the data subject's consent for one or more specific processing purposes. (Article 6(1)(a), GDPR.) For more on:

- When the GDPR requires data subject consent, including valid consent elements, documentation, and withdrawing consent, see Country Q&A, Data Protection in the EU: Overview: Question 9 and Practice Notes:
  - Overview of EU General Data Protection Regulation: Consent requirements; and
  - Demonstrating Compliance with the GDPR.
- The other legal grounds for processing personal data:
  - in Greece, see Question 10.
  - under the GDPR, see Country Q&A, Data Protection in the EU: Overview: Question 10.

The Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) does not specify, restrict, or expand the GDPR's requirements for consent.

Explicit Consent

The GDPR requires controllers relying on consent as the legal basis for processing personal data to obtain explicit consent in certain circumstances (see Country Q&A, Data Protection in the EU: Overview: Question 10). GDPR Article 9(2)(a) permits EU or member state law to prohibit the use of explicit data subject consent as a legal basis for processing special categories of personal data. The Data Protection Law does not prohibit this.

The Data Protection Law also requires explicit data subject consent to process personal data for journalistic purposes or academic, artistic, or literary expression (Article 28(1), Data Protection Law).

Consent by Minors

For online service providers offering services directly to children (called information society services in the GDPR), the GDPR permits EU member states to lower the age of child consent below 16 years old, if the age is not lower than 13 (Article 8(1), GDPR). The Data Protection Law lowers the age of child consent to 15 (Article 21, Data Protection Law). The Data Protection Law does not otherwise change the requirements for obtaining valid consent from children or impose any additional requirements or restrictions on processing personal data about children.

10. If consent is not given, on what other grounds (if any) can processing be justified?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1). The GDPR permits personal data processing without data subject consent if at least one of the following other legal bases for processing applies:

- The processing is necessary to enter into or perform a contract with the data subject or to take pre-contractual steps at the data subject's request.
- The processing is necessary for the controller to comply with a legal obligation.
- The processing is necessary to protect the vital interests of the data subject or another natural person.
- The processing is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the controller.
- The processing is necessary to pursue the controller's or a third party's legitimate interests, unless the data subject's interests or fundamental rights and freedoms override those interests.

(Article 6(1), GDPR.)

Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) permits public bodies to process personal data where processing is necessary to perform a task carried out in the public interest or in the exercise of official authority conferred on the controller (Article 5, Data Protection Law).

Articles 24 and 25 of the Data Protection Law also permit secondary processing by public and private bodies in certain circumstances. However, the Hellenic Data Protection Authority has indicated they will not apply those provisions because they do not align with the GDPR (see Question 8). Otherwise, the Data Protection Law generally does not modify the GDPR's legal bases for processing.

A controller may process special categories of personal data without the data subject's prior consent if the processing meets certain requirements (see Question 11).

For more on consent as a legal basis for personal data processing, see Question 9. For more on lawful bases for processing, see Practice Note, Demonstrating Compliance with the GDPR: Lawfulness of Processing.

Special Rules

11. Do special rules apply for certain types of personal data, such as sensitive data?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1) and:

- Prohibits processing special categories of personal data, previously known as sensitive data under the GDPR, unless an exception applies (Article 9, GDPR).
- Allows EU member states to introduce further conditions and limitations on processing genetic, biometric, and health data (Article 9(4), GDPR).
- Limits who may process personal data relating to criminal conviction and offenses and when this processing may occur (Article 10, GDPR).

Like the GDPR, Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) prohibits processing special categories of personal data unless an exception applies (Article 9(1), GDPR; Article 22, Data Protection Law).

For more on processing special categories of personal data under the GDPR, see Country Q&A, Data Protection in the EU: Overview: Question 11.

Special Categories of Personal Data

Under the GDPR, special categories of personal data include personal data revealing any of the following:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data to uniquely identify a natural person.
- Data concerning a natural person's:
    - health;
    - sex life; or
    - sexual orientation.

(Article 9, GDPR.)

The Data Protection Law permits:

- Public and private bodies to process special categories of personal data without data subject consent when necessary:
    - to exercise rights arising from the right to social security and social protection and to fulfil related obligations;
    - for preventive medicine, assessing an employee's working capacity, medical diagnosis, the provision of health and social care, the management of health or social care systems and services, or under a contract with a health professional or other person subject to a professional secrecy obligation; or
    - for public interest reasons in the area of public health.

- Public bodies to process special categories of personal data without data subject consent only:
    - in cases of public interest;
    - to prevent a significant threat to public safety; or
    - to take humanitarian measures.

(Article 22, Data Protection Law.)

The Data Protection Law sets out special rules for processing special categories of personal data for secondary purposes. To process special categories of personal data for secondary purposes, controllers must:

- Fulfill the conditions in Data Protection Law Articles 24(1) and 25(1) (see Question 8).
- Qualify for one of the exceptions permitting processing special categories of personal data under GDPR Article 9(2) or Data Protection Law Article 22.

(Articles 24(2) and 25(2), Data Protection Law.)

Under the Data Protection Law, controllers may be permitted to process special categories of personal data in specific processing situations, including when processing:

For archiving in the public interest (Article 29(1), Data Protection Law).

For scientific or historical research purposes or statistical purposes (Article 30(1), Data Protection Law).

- In the employment context if both:
    - the processing is necessary for the employer to exercise its rights or comply with legal obligations arising from employment, social security, and social protection law; and
    - there is no reason to believe that the data subject's legitimate interests in relation to processing take precedence.

    (Article 27(3), Data Protection Law.) However, the HDPA recommends, in accordance with case law, that controllers base certain employment-related processing, including biometric data processing, using

geolocation systems, drafting electronic monitoring regulations, and using whistleblowing systems, on GDPR Article 6(1)(e) (processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) or Article 6(1)(f) (processing necessary for the purposes of a legitimate interest). This allows employees to challenge separate processing activities and assert their rights under GDPR without the employer challenging the terms of their employment contract. (HDPA: Opinion 1/2020 (in Greek).)

These specific processing situations may also affect data subject rights (see Question 12 and Question 13). For more on these specific processing situations, see Practice note, Greek Implementation of the GDPR: Derogations for Specific Processing Situations.)

For more on security requirements when processing special categories of personal data, see Question 15.

Genetic, Biometric, and Health Data

The GDPR permits EU member states to introduce further conditions and limitations on processing genetic, biometric, and health data (Article 9(4), GDPR). The Data Protection Law prohibits genetic data collection and processing for health and life insurance purposes (Article 23, Data Protection Law). According to HDPA Opinion 1/2020 (in Greek), genetic data collection and processing for employment purposes is also prohibited.

Criminal Conviction and Offense Data

The GDPR only permits processing personal data relating to criminal convictions and offenses when either:

- Carried out under the control of an official authority, for example, the police.
- EU or EU member state law authorizes the processing and provides for appropriate safeguards for data subjects' rights and freedoms.

(Article 10, GDPR.)

The Data Protection Law permits processing personal data relating to criminal proceedings and convictions and related security measures for journalistic purposes or purposes of academic, artistic, or literary expression, provided the controller both:

- Limits processing to what is necessary to ensure freedom of expression and the right to information.
- Considers the data subject's right to private and family life.

(Article 28, Data Protection Law; see HDPA Opinion 1/2020 (in Greek)).

For more on processing:

- Non-special categories of personal data, see Question 4.
- Special categories of personal data, see Practice Note, Overview of EU General Data Protection Regulation: Special Categories of Personal Data.

Rights of Individuals

12. What information rights do data subjects have?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1) and requires controllers to provide data subjects with certain information at the point of collection depending on whether they collect the personal data directly from the data subject or from a third party (Articles 13 and 14, GDPR). The information controllers must provide in each case is similar, but not identical. For more on what information the GDPR requires in each of these circumstances, see Country Q&A, Data Protection in the EU: Overview: Question 12 and Practice note, Data Subject Rights Under the GDPR: Information Right.

EU member states may restrict the scope of data subjects' information rights and controllers' related obligations under GDPR Articles 13, 14, and 5 (as it relates to the rights and obligations in Articles 13 and 14) when the restriction is a necessary and proportionate measure to safeguard GDPR Article 23 objectives or in other specific processing situations (Articles 23 and 85, GDPR; for more on other specific data subject rights and the GDPR Article 23 objectives, see Question 13).

Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) permits controllers to restrict data subjects' information rights under GDPR Article 13(3), which requires the controller, when it intends to further process personal data for a new purpose, to provide information to the data subject before further processing the personal data. Under the Data Protection Law, GDPR Article 13(3) does not apply:

- To further processing when:
    - the processing concerns data the controller stores in a written form which directly addresses the data subject;
    - the processing has a compatible purpose with the original collection purpose under GDPR Article 6(4);
    - the controller does not communicate with the data subject in digital form; and
    - the data subject does not have a significant interest in being informed in the specific circumstances, given the context of the data collection.
- To further processing by public bodies when:
    - providing the information would compromise the proper performance of the controller's tasks under GDPR Article 23(1)(a) to (e); and
    - the controller's interest in not providing the information overrides that data subject's interest.

- When providing the information would:
    - compromise national or public security, and the controller's interest in not providing the information overrides the data subject's interest;
    - prevent the establishment, exercise, or defense of legal claims, and the controller's interest in not providing the information overrides the data subject's interest; or
    - compromise the confidentiality of a data transfer to a public body.

(Article 31(1), Data Protection Law.)

The Data Protection Law also permits controllers to restrict data subjects' information rights under GDPR Article 14, which requires the controller to inform data subjects when it obtains their personal data from a third party. Under the Data Protection Law, GDPR Article 14(1), (2), and (4) do not apply:

- To public bodies when notifying the data subject would compromise:
    - the controller's proper performance of its tasks under GDPR Article 23(1)(a) to (e); or
    - national or public security and the controller's interests override the data subject's information rights.

- To private bodies when:
    - notification would prejudice the establishment, exercise, or defense of legal claims;
    - the processing includes personal data resulting from contracts established under private law and is aimed at preventing damages caused by criminal offenses, unless the data subject has an overriding legitimate interest in obtaining the information; or
    - the competent public authority specifies to the controller that publishing the personal data would compromise national defense, national security, and public security.

(Article 32(1), Data Protection Law.)

The Data Protection Law also does not require controllers to provide information to the data subject under GDPR Article 14(1) to (4) if doing so would disclose information that, due to a third party's overriding legitimate interests, should remain confidential (Article 32(3), Data Protection Law).

Controllers are subject to additional requirements when they do not provide information to data subjects under Data Protection Law Articles 31 and 32.

The Data Protection Law permits controllers to restrict data subjects' information rights under GDPR Articles 12 to 14 to the extent necessary to reconcile the right to data protection with the right to freedom of expression and information, including when processing for journalistic purposes or academic, artistic, or literary expression (Article 28(2), Data Protection Law). For more, see Practice note, Greek Implementation of the GDPR: Processing for Journalistic Purposes and Academic, Artistic, or Literary Expression.

For more on other data subject rights, see Question 13.

13. Other than information rights, what other specific rights are granted to data subjects?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) applies directly in Greece (see Question 1). For more on individual data subject rights under the GDPR and handling data subject requests, see:

- Country Q&A, Data Protection in the EU: Overview: Question 13.
- Practice Notes:
  - Complying with the GDPR's Transparency Obligation to Data Subjects; and
  - Data Subject Rights Under the GDPR.
- Responding to Data Subject Requests Under the GDPR Checklist.
- Handling Data Subject Requests Under the GDPR Toolkit.

Data Subject Rights Derogations

EU member states may restrict the scope of data subjects' rights and controllers' related obligations in GDPR Articles 12 to 22, 34, and 5 (as it relates to the rights and obligations in Articles 12 to 22) when the restriction is a necessary and proportionate measure to safeguard:

- National security.
- Defense.
- Public security.
- The prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties.
- Other important economic or financial public interests of the EU or EU member state, including:
  - monetary, budgetary, and taxation matters;
  - public health; and
  - social security.
- Judicial independence and proceedings.
- The prevention, investigation, detection, and prosecution of ethics breaches for regulated professions.

- Monitoring, inspection, or regulatory functions connected to the exercise of official authority regarding:
  - national or public security;
  - defense;
  - other important public interests;
  - crime prevention; or
  - breaches of ethics for regulated professions.
- Protection of the individual or the rights and freedoms of others.
- Enforcing civil law matters.

(Article 23(1), GDPR.)

Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) varies certain data subject rights or related controller or processor obligations when necessary to safeguard GDPR Article 23 objectives. For an in-depth discussion of these derogations, including in specific processing situations, see Practice note, Greek Implementation of the GDPR: Data Protection Law Variations to Data Subject Rights and Derogations for Specific Processing Situations.

The Hellenic Data Protection Authority (HDPA) has stated that Data Protection Law Articles 31 to 35 provide extensive restrictions on data subject rights without specifically citing GDPR Article 23(4). The HDPA explicitly reserved judgment on the compatibility of these restrictions with the GDPR, the EU Charter of Fundamental Rights, and the European Convention on Human Rights. (HDPA: Opinion 1/2020 (in Greek).)

14. Do data subjects have a right to request the deletion of their data?

See Question 13.

Security Requirements

15. What security requirements are imposed in relation to personal data?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1). For more on the GDPR's security requirements for controllers and processors, see Country Q&A, Data Protection in the EU: Overview: Question 15.

Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) does not specify, restrict, or expand the GDPR's general data security requirements.

Controllers processing special categories of personal data must take appropriate and specific measures to safeguard data subject's interests, taking into account available technology, implementation costs, the processing's nature, scope, and purposes, and the severity of risk to natural persons' rights and freedoms that the processing poses. This may include:

- Technical and organizational measures to ensure the processing complies with the GDPR.
- Measures to:
    - ensure the controller can verify after the fact if and who entered, amended, or removed personal data;
    - raise awareness for staff involved in the processing;
    - restrict access; and
    - ensure processing systems' ability, confidentiality, integrity, availability, and resilience, including the ability to rapidly restore availability and access after a physical or technical incident.
- Pseudonymization and encryption of personal data.
- Procedures to regularly test, assess, and evaluate the effectiveness of technical and organizational measures to ensure processing security.
- Specific rules to ensure compliance with the Data Protection Law and the GDPR when transferring personal data or processing for other purposes.
- Designating a data protection officer.

(Article 22(3), Data Protection Law.)

16. Is there a requirement to notify data subjects or the supervisory authority about personal data security breaches?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1). For more on the GDPR's requirements to notify supervisory authorities and data subjects about certain data breaches, see Country Q&A, Data Protection in the EU: Overview: Question 16.

Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) permits controllers to restrict data subjects' breach notification right under GDPR Article 34 when notification would require the disclosing information that should remain confidential by law or by its nature, in particular due to third parties' overriding legitimate interests, unless the data subject's interests, in particular any imminent damage, override the interest in maintaining confidentiality (Article 33(5), Data Protection Law).

The Hellenic Data Protection Authority (HDPA) requires controllers to report data breaches electronically via its online portal (HDPA: Submission of notification of a violation incident to the Authority (in Greek)).

Sectoral laws may also impose additional breach notification requirements, but these laws are outside the scope of this Q&A.

Processing by Third Parties

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1). For more on the GDPR's requirements when engaging processors, see Country Q&A, Data Protection in the EU: Overview: Question 17.

Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) allows public bodies to transfer personal data to other public bodies where necessary to perform either party's tasks. The third-party transferee may only process the data for the purpose for which the transferor sent it. Any further processing must meet the conditions set out in Data Protection Law Article 24. (Article 26(1), Data Protection Law; see Question 8.)

Public bodies may transfer personal data to private bodies if one of the following conditions is met:

- The transfer:
    - is necessary for the public body to perform its tasks; and
    - meets the conditions for secondary processing set out in Data Protection Law Article 24.
- The private body receiving the data has a legitimate interest in the transfer, and the data subject does not have a legitimate interest in not transferring the data.
- The processing is necessary to establish, exercise, or defend a legal claim, and the private body receiving the data agrees to use it only for the purpose for which the public body sent it. Processing for other purposes:
    - must comply with Data Protection Law Article 26(1) as discussed above; and

- requires the transferring body's consent.

(Article 26(2), Data Protection Law.)

Public bodies may transfer special categories of personal data if additional conditions are met (Article 22, Data Protection Law; see Question 11).

Controllers may also need to meet additional requirements for cross-border data transfers (see Question 20).

Electronic Communications

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), which applies directly in Greece (see Question 1), does not expressly address the use of cookies or equivalent devices.

For more on:

- The GDPR's requirements regarding cookies, including the need for a legal basis for processing, see Country Q&A, Data Protection in the EU: Overview: Question 18.
- The status of the Proposed E-Privacy Regulation, see Digital Single Market Strategy: Regulation on Privacy and Electronic Communications (ePrivacy Regulation): legislation tracker.
- How EU member states regulate cookies, see EU Member State Cookie Directive Implementation Chart.

Law 3471/2006 on the Protection of Personal Data and Privacy in the Electronic Telecommunications Sector, as amended (in Greek) (E-Privacy Law) regulates the use of cookies or equivalent devices in Greece and generally requires subscribers or users to consent (opt-in) after receiving clear and comprehensive information about cookie use (Article 4(5), E-Privacy Law). Further details of the E-Privacy Law are outside the scope of this Q&A.

The Hellenic Data Protection Authority has issued recommendations to help controllers comply with legal requirements for the use of cookies (HDPA: Recommendations for data controllers to comply with specific electronic communications legislation (February 25, 2020) (in Greek)).

19. What rules regulate sending commercial or direct marketing communications?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), which applies directly in Greece (see Question 1), does not expressly address the sending of unsolicited electronic commercial communications (spam), but it does give data subjects the right to object to personal data processing for direct marketing purposes (Article 21(3), GDPR). For more on sending spam under the GDPR and the requirement for a legal basis for processing, see Country Q&A, Data Protection in the EU: Overview: Question 19.

Law 3471/2006 on the Protection of Personal Data and Privacy in the Electronic Telecommunications Sector, as amended (in Greek) (E-Privacy Law) prohibits unsolicited direct marketing of goods or services through email without the recipient's explicit consent (Article 11, E-Privacy Law). Further details of the E-Privacy Law are outside the scope of this Q&A.

The Hellenic Data Protection Authority published additional guidance on obtaining consent under the E-Privacy Law (HDPA: Directive 2/2011 on Consent Given via Electronic Means (March 29, 2011) (in Greek)).

International Transfer of Data

Transfer of Data Outside the Jurisdiction

20. What rules regulate the transfer of data outside your jurisdiction?

The EU General Data Protection Regulation (Regulation (EU) 679/2016) (GDPR) applies directly in Greece (see Question 1). The GDPR allows controllers and processors to transfer personal data within the European Economic Area (EEA) if a lawful basis for the processing exists (see Question 9 and Question 10). Otherwise, it only allows for transfers of personal data outside of the EEA to third countries and international organizations based on:

- Adequacy decisions.
- Appropriate safeguards, such as standard contract clauses and binding corporate rules.
- Derogations from the general prohibition.
- Nonrepetitive transfers.

(Articles 44 to 50, GDPR.)

For more on cross-border transfers under the GDPR, see Country Q&A, Data Protection in the EU: Overview: Question 20.

The GDPR allows EU member states to, for important public interest reasons, enact national laws limiting the cross-border transfer of specific categories of personal data if the destination country has not been deemed to provide an adequate level of data protection (Article 49(5), GDPR). Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data does not address GDPR Article 49(5).

For more on:

- Cross-border data transfer agreements, see Question 22.
- Regulatory guidance after the EU Court of Justice's (ECJ) ruling in *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (Case C-311/18) EU:C:2020:559* (Schrems II), see *EU Cross-Border Data Transfers: Regulatory Guidance Post Schrems II Tracker*.
- General and country-specific resources to help organizations comply with data protection laws when transferring personal data across borders, see Cross-Border Personal Data Transfers Toolkit.

21. Is there a requirement to store any type of personal data inside the jurisdiction?

Neither the EU General Data Protection Regulation (Regulation (EU) 2016/679) nor Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data requires controllers to store any type of personal data in any specific jurisdiction.

Sector-specific Greek laws may impose data localization requirements. These laws are outside the scope of this Q&A.

Data Transfer Agreements

22. Are data transfer agreements contemplated or in use? Has the supervisory authority approved any standard forms or precedents for cross-border transfers?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1). For cross-border data transfers to third countries without an adequacy decision, controllers can meet the GDPR's requirements by using data transfer agreements, such as:

- Standard contractual clauses that the European Commission (EC) has adopted.

- Standard contractual clauses that a national supervisory authority has adopted and that the EC has approved.
- Other contractual clauses that a competent national supervisory authority has authorized.

(Article 46(2), (3), GDPR.)

The Hellenic Data Protection Authority has not approved any standard forms or precedents for cross-border transfers.

For more on rules regulating cross-border data transfers in Greece and the EU respectively, including other possible mechanisms to legally transfer data, see Question 20 and Country Q&A, Data Protection in the EU: Overview: Question 20 and Question 22.

23. For cross-border transfers, is a data transfer agreement sufficient, by itself, to legitimize transfer?

See Question 20 and Question 22.

24. Must the relevant supervisory authority approve the data transfer agreement for cross-border transfers?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1). The Hellenic Data Protection Authority (HDPA) does not need to approve a data transfer agreement that uses unamended Standard Contractual Clauses (SCCs). However, the HDPA must approve data transfer agreements that amend or supplement SCCs in a way that directly or indirectly contradicts the measures provided for in the SCCs (Article 46(3), GDPR).

The HDPA has also issued guidance after the EU Court of Justice's (ECJ) July 16, 2020 ruling in Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (Case C-311/18) EU:C:2020:559 (Schrems II). For more, see EU Cross-Border Data Transfers: Regulatory Guidance Post Schrems II Tracker.

For more information on the HDPA's notification, registration, or authorization requirements before transferring personal data cross-border, see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: Greece: Questions 2 and 3.

For the HDPA's contact information, see Regulator Details.

Enforcement and Sanctions

25. What are the enforcement powers of the supervisory authority?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1). For more on the enforcement powers supervisory authorities have under the GDPR, see Country Q&A, Data Protection in the EU: Overview: Question 25.

GDPR Article 54 requires each EU member state to establish a supervisory authority. Articles 9 to 20 of Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) establish the Hellenic Data Protection Authority's (HDPA) structure, organization, tasks, and powers. In addition to the duties under GDPR Article 57, the HDPA, among other things:

- Monitors and enforces the Data Protection Law and other regulations related to personal data protection and processing.
- Promotes public awareness and understanding of the risks, safeguards, and rights related to personal data processing.
- Provides opinions on draft laws and regulatory acts related to personal data processing.
- Issues guidelines and makes recommendations on matters related to personal data processing.
- Informs data subjects how to exercise their rights under the Data Protection Law on specific request.
- Issues standard documents and complaint forms.
- Handles complaints that data subjects or other bodies, organizations, or associations lodge and inform complainants of the progress and outcome within a reasonable time.
- Conducts investigations or inspections initiated on its own or after a complaint, on the application of the Data Protection Law and other regulations related to personal data protection and processing.
- Monitors relevant personal data protection developments, in particular developments in information and communication technologies and commercial practices.
- Contributes to the European Data Protection Board's activities.
- Submits a yearly report of its activities to the President of the Parliament and the Prime Minister.

(Articles 13 and 14, Data Protection Law.)

In addition to its powers under GDPR Article 58, the HDPA has the power to:

- Conduct investigations and audits initiated on its own or after a complaint, relating to Data Protection Law compliance when the technological infrastructure and other automated or non-automated means supporting personal data processing are subject to controls.
- Issue corrective actions, including warnings, compliance orders, temporary or final limitations, bans, and inspection and seizure orders.
- Order a controller, processor, recipient, or third party to:
    - discontinue personal data processing;
    - return or block relevant data; or
    - destroy a filing system or relevant data.

(Article 15, Data Protection Law.)

For more on sanctions and remedies for non-compliance with the Data Protection Law, see Question 26.

26.What are the sanctions and remedies for non-compliance with data protection laws?

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Question 1). For more on the GDPR's enforcement and applicable sanctions, see Country Q&A, Data Protection in the EU: Overview: Question 26 and Practice Note, Enforcement, Sanctions, and Remedies under the GDPR.

The GDPR permits EU member states to specify whether and to what extent supervisory authorities may impose administrative fines on public authorities and bodies (Article 83(7), GDPR). Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) makes use of this derogation and imposes administrative sanctions up to EUR10 million on public bodies that violate specific GDPR provisions (Article 39(1), Data Protection Law). Data Protection Law Article 39(2) lists factors the Hellenic Data Protection Authority (HDPA) should consider when assessing administrative penalties. The Data Protection Law does not address further administrative fines for private bodies.

In addition to the fines applicable under GDPR Article 83, the GDPR permits EU member states to specify penalties applicable to GDPR violations that are not subject to administrative fines under this article (Article 84, GDPR). The Data Protection Law imposes criminal penalties for specific personal data violations, including up to ten years' imprisonment and fines between EUR100,000 and EUR300,000 depending on the type and severity of the violation (Article 38, Data Protection Law).

For key Greek enforcement actions relating to GDPR violations, see Practice Note, GDPR Enforcement Tracker by Country (EEA): Greece.

Regulator Details

Hellenic Data Protection Authority

T +30 210 6475600

F +30 210 6475628

E contact@dpa.gr

W www.dpa.gr (in Greek and English)

Main areas of responsibility. Enforcement of information security standards and regulations, including those related to personal data protection.

Contributor Profiles

Popi Papantoniou, Senior Associate

Bahas, Gramatidis & Partners LLP
T + 30 210 3318170

F + 30 210 3318171

E p.papantoniou@bahagram.com

W https://www.bahagram.com/attorneys/senior-associates/popi-papantoniou/

Professional qualifications. Greece, Attorney

Areas of practice. Civil law; commercial/corporate law and commercial litigation; data protection; information technology law.

Valeria Kokkinou, Junior Associate

Bahas, Gramatidis & Partners LLP
T + 30 210 3318170

F + 30 210 3318171

E v.kokkinou@bahagram.com

W www.bahagram.com

Professional qualifications. Greece, Attorney

Areas of practice. Civil, commercial, and personal data protection law.

END OF DOCUMENT

