GDPR Derogations: Greece

by Tania Patsalia and Vangelis Kalogiannis, Bernitsas Law Firm, with Practical Law Data Privacy Advisor

Country Q&A | Law stated as of 01-Jun-2021 | Greece, International

A Q&A providing jurisdiction-specific commentary on the Greek implementation of the GDPR, including key derogations from the GDPR's requirements. For information on topics not addressed in this Q&A, see Practice note, Greek Implementation of the GDPR.

Applicable Law

1. What laws in your country implement the GDPR?

Greece enacted Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law), which supplements the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) and further specifies some of its requirements. Specific provisions of the prior Law 2472/1997 on the Protection of Individuals Regarding Processing Personal Data remain effective (Article 84, Data Protection Law).

The Hellenic Data Protection Authority (HDPA) has also issued:

- Opinion 1/2020 (January 24, 2020) (in Greek) (HDPA Opinion 1/2020) to clarify the Data Protection Law's compatibility with the GDPR.
- Guidance and opinions (in Greek) on personal data protection and processing under the Data Protection Directive and Law 2472/1997. According to the HDPA, this guidance remains in force and applies in parallel with the GDPR and the Data Protection Law to the extent it does not conflict with the GDPR.

Scope

2. What is the territorial scope of the GDPR-implementing law?

The Greek Data Protection Law's territorial scope provision 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).

Data Protection Officers

3. **(Article 37(4), GDPR)** Under what additional circumstances does the law require a data protection officer?

The Greek Data Protection Law includes provisions on the appointment of data protection officers (DPOs) in public bodies (Articles 6 to 8, Data Protection Law).

4. **(Article 38(5), GDPR)** Does the law bind data protection officers to secrecy obligations or subject them to different requirements or obligations than the GDPR?

Yes. Under the Greek Data Protection Law, public body data protection officers (DPOs) are bound to maintain the confidentiality of the data subject's identity, unless the data subject discloses their own identity (Article 7(5), Data Protection Law).

A public body DPO who becomes aware of personal data while performing their tasks may refuse to give evidence as a witness for professional reasons if the public body's head would also have the right to refuse. This right also applies to the DPO's assistants. (Article 7(6), Data Protection Law.)

Special Categories of Personal Data

5. **(Article 9(2), GDPR)** Does the law permit processing special categories of personal data?

Yes. The Greek Data Protection Law permits:

- Public and private bodies to process special categories of personal data 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 only:
    - in cases of substantial public interest;
    - when necessary to prevent a significant threat to national security or public safety; or
    - when necessary to take humanitarian measures, so long as the processing overrides the data subject's interest.

(Article 22, Data Protection Law.)

The Data Protection Law also allows employers to process special categories of personal data if they meet certain conditions (see Question 23).

Controllers processing special categories of personal data based on the above exceptions must take appropriate and specific measures to safeguard data subjects' 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.)

The Data Protection Law also permits processing special categories of personal data under certain conditions for:

- Secondary purposes (Articles 24(2) and 25(2), Data Protection Law; see Question 10).
- Freedom of expression and information (Article 28, Data Protection Law; see Question 17).
- Archiving in the public interest (Article 29(1), Data Protection Law; see Question 20).
- Scientific or historical research or statistical purposes (Article 30(1), Data Protection Law, see Question 20).

6. **(Article 9(2)(a), GDPR)** Does the law prohibit the use of explicit data subject consent as a legal basis for processing special categories of personal data?

No. The Greek Data Protection Law does not prohibit the use of explicit consent as a legal basis for processing special categories of personal data.

7. **(Article 9(4), GDPR)** Does the law impose any further conditions or limitations on processing genetic, biometric, or health-related data?

Yes. The Greek Data Protection Law prohibits collecting and processing genetic data for health and life insurance purposes (Article 23, Data Protection Law). According to the Hellenic Data Protection Authority's Opinion 1/2020, any prohibition on processing genetic data extends to processing in the employment context (see Question 23).

8. Does the law require specific security measures to protect special categories of personal data that are different than or in addition to those required by the GDPR?

Yes. Controllers operating in Greece who process special categories of personal data based on the exceptions set out in Question 5 must take appropriate and specific measures to safeguard data subjects' 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.)

Criminal Conviction and Offense Data

9. **(Article 10, GDPR)** Does the law permit processing criminal conviction and offense data? If yes, under what circumstances?

Yes. The Greek Data Protection Law does not explicitly address processing criminal conviction and offense data or permitted processing purposes. However, it references controllers processing personal data relating to criminal proceedings and convictions and related security measures to ensure freedom of expression and the right to information, provided they both:

- Limit processing to what is necessary for the processing purpose.
- Consider the data subject's right to private and family life.

(Article 28, Data Protection Law; see Hellenic Data Protection Authority Opinion 1/2020.)

Secondary Processing Purposes

10. **(Article 6(4), GDPR)** Does the law permit processing for secondary purposes?

Yes. The Greek Data Protection Law permits:

- 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 the Hellenic Data Protection Authority (HDPA), Articles 24 and 25 establish bases to process personal data for purposes other than initially collected (see HDPA Opinion 1/2020). 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, Articles 24 and 25 are not in line with the GDPR.

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), as set out above.
- Qualify for one of the exceptions permitting processing special categories of personal data under GDPR Article 9(2) or Data Protection Law Article 22 (see Question 5).

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

Child Consent

11. **(Article 8(1), GDPR)** Does the law lower the age of consent for children?

Yes. The Greek Data Protection Law lowers the age of child consent to 15 (Article 21, Data Protection Law).

12. Does the law change the requirements for obtaining a child's consent or impose any restrictions or limitations on processing children's personal data?

No. The Greek Data Protection Law does not change the requirements for obtaining valid consent from children or impose any additional requirements or restrictions on processing personal data about children.

Data Subjects' Rights

13. **(Articles 12 to 17, GDPR)** Does the law limit or change the scope of data subjects' information (Articles 12 to 14, GDPR), access (Article 15, GDPR), rectification (Article 16, GDPR), or erasure rights (Article 17, GDPR)?

Yes. The Greek Data Protection Law varies the following data subject rights or related controller or processor obligations when necessary to safeguard GDPR Article 23 objectives:

- Information rights (see Information Right).
- Access rights (see Access Right).
- Rectification rights (see Rectification Right).
- Erasure rights (see Erasure Right).

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.)

Information Right

The Data Protection Law permits controllers to restrict data subjects' information rights under GDPR Article 13(3), which requires controllers that intend to further process personal data for a new purpose to inform the data subject in advance. Under the Data Protection Law, GDPR Article 13(3) does not apply:

- To further processing when:
    - the processing concerns personal data the controller stores in a written form which directly addresses the data subject;
    - the processing is compatible 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 controller's proper performance its tasks under GDPR Article 23(1)(a) to (e); and
    - the controller's interest in not providing the information overrides the 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 that do not provide information to data subjects must:

- Take appropriate measures to protect the data subjects' legitimate interests.

- In most cases, notify the data subject in writing of their reasons for not providing the information.

(Articles 31(2) and 32(2), Data Protection Law.)

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; see Question 17).

Access Right

The Data Protection Law permits controllers to restrict data subjects' access right under GDPR Article 15:

- To the extent necessary to reconcile the right to data protection with the right to freedom of expression and information, including processing for journalistic purposes or academic, artistic, or literary expression (Article 28(2), Data Protection Law; see Question 17).
- When allowing the data subject to exercise the access right likely renders impossible or seriously impairs the objectives of processing for archiving purposes in the public interest and exercising the right would require a disproportionate effort (Article 29(2), Data Protection Law; see Question 20).
- When allowing the data subject to exercise the access right likely renders impossible or seriously impairs the objectives of processing for scientific or historical research or for statistical purposes, and:
    - restricting the right is necessary to achieve those purposes; and
    - providing the information would require a disproportionate effort.

    (Article 30(2), Data Protection Law; see Question 20.)
- In certain circumstances where data subjects' information rights are also restricted under Data Protection Law Article 32(a)(bb) and (b)(bb) (Article 33(1)(a), Data Protection Law).
- When the controller recorded the personal data because of retention requirements under another legal or regulatory provision (Article 33(1)(b)(aa), Data Protection Law).
- When the personal data's only purpose is data control or protection, and:
    - providing access would require disproportionate effort; and
    - the controller has implemented necessary technical and organizational measures to render processing for other purposes impossible.

    (Article 33(1)(b)(bb), Data Protection Law.)
- When the information to be disclosed to the data subject should remain confidential by law or by its nature, in particular due to third parties' overriding legitimate interests (Article 33(4), Data Protection Law).

In addition, a data subject's right to access personal data stored in a filing system that is not subject to a public authority's automated or non-automated processing only applies if both:

- The data subject provides information allowing retrieval of the data.
- The effort required to provide the information is not disproportionate to the data subject's interest in being informed.

(Article 33(3), Data Protection Law.)

Rectification Right

The Data Protection Law permits controllers to restrict data subjects' rectification right under GDPR Article 16:

- To the extent necessary to reconcile the right to data protection with the right to freedom of expression and information, including processing for journalistic purposes or academic, artistic, or literary expression (Article 28(2), Data Protection Law; see Question 17).
- When allowing the data subject to exercise the right likely renders impossible or seriously impairs:
    - the objectives of processing for archiving purposes in the public interest; or
    - the exercise of the rights of others.

    (Article 29(3), Data Protection Law.)
- When allowing the data subject to exercise the right likely renders impossible or seriously impairs the objectives of processing for scientific or historical research or for statistical purposes and restricting the right is necessary to achieve those purposes (Article 30(2), Data Protection Law; see Question 20).

Erasure Right

The Data Protection Law permits controllers to restrict data subjects' erasure right under GDPR Article 17:

- 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; see Question 17).
- For non-automated processing, if erasure is not possible due to the particular nature of the storage or is only possible with disproportionate effort and the data subject's interest in erasure is not significant, unless one of the exceptions to the erasure right in GDPR Article 17(3) applies. In that case, the data subject's restriction right under GDPR Article 18 replaces the erasure right. This does not apply for unlawfully processed personal data. (Article 34(1), Data Protection Law.)
- For non-automated processing, when the controller no longer needs the personal data for the collection purpose under GDPR Article 17(1)(a) or the personal data was unlawfully processed under GDPR Article 17(1)(d), but the controller has reason to believe that erasure would be prejudicial to the data subject's legitimate interests. In that case, the data subject's restriction right under GDPR Article 18 replaces the erasure right. (Article 34(2), Data Protection Law.)

- For non-automated processing, when the controller no longer needs the personal data for the collection purpose under GDPR Article 17(1)(a), but erasure would conflict with statutory or contractual retention periods. In that case, the data subject's restriction right under GDPR Article 18 replaces the erasure right. (Article 34(3), Data Protection Law.)

14. **(Articles 18 to 21, GDPR)** Does the law limit or change the scope of data subjects' objection (Article 21, GDPR), processing restriction (Article 18, GDPR), or data portability rights (Article 20, GDPR)?

Yes. The Greek Data Protection Law varies the following data subject rights or related controller or processor obligations when necessary to safeguard GDPR Article 23 objectives:

- Processing restriction rights (see Processing Restriction Right).
- The right to data portability (see Data Portability Right).
- The right to object to processing (see Objection Right).

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.)

Processing Restriction Right

The Data Protection Law permits controllers to restrict data subjects' right to restrict personal data processing under GDPR Article 18:

- 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; see Question 17).
- When allowing the data subject to exercise the right likely renders impossible or seriously impairs the objectives of processing for archiving purposes in the public interest and restricting the right is necessary to achieve those purposes (Article 29(4), Data Protection Law; see Question 20).
- When allowing the data subject to exercise the right likely renders impossible or seriously impairs the objectives of processing for scientific or historical research or for statistical purposes and restricting the right is necessary to achieve those purposes (Article 30(2), Data Protection Law; see Question 20).

Data Portability Right

The Data Protection Law permits controllers to restrict data subjects' right to data portability under GDPR Article 20:

- 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; see Question 17).
- When allowing the data subject to exercise the right likely renders impossible or seriously impairs the objectives of processing for archiving purposes in the public interest and restricting the right is necessary to achieve those purposes (Article 29(4), Data Protection Law; see Question 20).

Objection Right

The Data Protection Law permits controllers to restrict data subjects' objection right under GDPR Article 21:

- 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; see Question 17).
- When allowing the data subject to exercise the right likely renders impossible or seriously impairs the objectives of processing for archiving purposes in the public interest and restricting the right is necessary to achieve those purposes (Article 29(4), Data Protection Law; see Question 20).
- When allowing the data subject to exercise the right likely renders impossible or seriously impairs the objectives of processing for scientific or historical research or for statistical purposes and restricting the right is necessary to achieve those purposes (Article 30(2), Data Protection Law; Question 20).
- If a public body is concerned, and:
    - a compelling public interest in the processing overrides the data subject's interests; or
    - the processing is required by law.

    (Article 35, Data Protection Law.)

15. **(Article 22, GDPR)** Does the law limit or change the scope of a data subject's right to not be subject to automated decision-making?

No. The Greek Data Protection Law does not limit or change the scope of a data subject's right to not be subject to automated decision-making.

16. **(Article 34, GDPR)** Does the law limit or change the scope of a data subject's right to be notified of a data breach?

Yes. The Greek Data Protection Law permits controllers to restrict data subjects' breach notification right under GDPR Article 34 when notification would require 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).

Processing for Journalistic, Academic, Artistic, or Literary Expression Purposes

17. **(Article 85, GDPR)** Does the law include rules that apply to processing personal data for journalistic, academic, artistic, or literary expression purposes?

Yes. The Greek Data Protection Law permits processing 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, if:

- The data subject explicitly consents.
- The processing relates to personal data the data subject made public.
- The right to freedom of expression and information overrides personal data protection rights, especially in relation to:
    - subjects of general interest; or
    - public figures' personal data.
- The processing is restricted to the extent necessary for ensuring the freedom of expression and information, especially when involving special categories of personal data and criminal conviction and offense data, taking into account the data subject's right to privacy.

(Article 28(1), Data Protection Law.)

In addition, the following GDPR provisions 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.)

Processing for journalistic purposes or academic, artistic, or literary expression may affect several data subject rights (see Question 13 and Question 14).

Disclosure of Personal Data in Official Documents

18. **(Article 86, GDPR)** Does the law include rules on the disclosure of personal data in official documents?

No. The Greek Data Protection Law does not include rules applicable to the disclosure of personal data in official documents.

Processing Identification Numbers

19. **(Article 87, GDPR)** Does the law include rules on processing identification numbers?

No. The Greek Data Protection Law does not include rules applicable to processing identification numbers.

Processing for Archiving in the Public Interest or for Scientific, Historical Research, or Statistical Purposes

20. **(Article 89, GDPR)** Does the law include rules on processing personal data for archiving in the public interest or for scientific, historical research, or statistical purposes?

Yes. The Greek Data Protection Law introduces rules that apply to:

- Processing for archiving in the public interest (see Processing for Archiving in the Public Interest).
- Processing for scientific or historical research purposes or statistical purposes (see Processing for Scientific or Historical Research Purposes or Statistical Purposes).

Processing for Archiving in the Public Interest

The Data Protection Law permits processing special categories of personal data where necessary for archiving in the public interest. Controllers processing special categories of personal data for this purpose must take suitable and specific measures to protect data subject's legitimate interests. (Article 29(1), Data Protection Law; see Question 5.)

Processing for archiving in the public interest may affect several data subject rights (Article 29(2) to (4), Data Protection Law; see Question 13 and Question 14).

Processing for Scientific or Historical Research Purposes or Statistical Purposes

The Data Protection Law permits processing special categories of personal data **without** data subject consent if controllers meet both of the following conditions:

- The processing is necessary for:
  - scientific or historical research purposes; or
  - collecting and maintaining statistical information.
- The controller's interest overrides the data subject's interest in not having their personal data processed.

(Article 30(1), Data Protection Law.)

Controllers processing special categories of personal data for this purpose must take suitable and specific measures to protect data subject's legitimate interests (Article 30(1), Data Protection Law; see Question 5).

Processing for scientific or historical research purposes or statistical purposes may affect several data subject rights (Article 30(2) to (4), Data Protection Law; see Question 13 and Question 14).

Processing Related to Secrecy Obligations

21. **(Article 90, GDPR)** Does the law include rules on processing relating to obligations of secrecy?

Yes. The Greek Data Protection Law grants the Hellenic Data Protection Authority's (HDPA) the power to access all personal data processed and all information necessary to conduct audits and perform its tasks, regardless of a controller's or processor's confidentiality obligations (Article 15(1), Data Protection Law).

Processing by Churches or Religious Organizations

22. **(Article 91, GDPR)** Does the law include rules on processing by churches or religious organizations?

No. The Greek Data Protection Law does not include rules applicable to processing by churches or religious organizations.

Processing Personal Data in the Employment Context

23. **(Article 88, GDPR)** Does the law include specific rules for processing personal data in the employment context? Are there any other laws in your country that apply to employee data processing (for example, labor laws)?

Yes. The Greek Data Protection Law permits employers to process employees' personal data for an employment contract if the processing is strictly necessary for:

- Deciding whether to enter into the contract.

- Performing the contract once entered into.

(Article 27(1), Data Protection Law.)

According to the Hellenic Data Protection Authority (HDPA), it is unclear whether Data Protection Law Article 27(1) repeats GDPR Article 6(1)(b) (processing necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering into a contract) or introduces a separate legal basis for processing personal data in the employment context. In either case, the HDPA considers Data Protection Law Article 27(1) not in line with the GDPR. (HDPA Opinion 1/2020.)

The Data Protection Law also permits employers to process special categories of personal data in the employment context if they meet both of the following conditions:

- 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.
- There is no reason to believe that the data subject's legitimate interests in relation to the processing override the controller's interests.

(Article 27(3), Data Protection Law.)

The Data Protection Law prohibits collecting and processing genetic data for health and life insurance purposes, which according to the HDPA's interpretation extends to processing in the employment context (Article 23, Data Protection Law and HDPA Opinion 1/2020; see Question 23).

Controllers are also permitted to process personal data, including special categories of personal data, for an employment contract based on collective labor agreements. Negotiating parties must comply with GDPR Article 88(2). (Article 27(4), Data Protection Law.)

The HDPA recommends, in accordance with case law, that controllers base certain employment-related processing, including processing biometric data, 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 the GDPR without the employer challenging the terms of their employment contract. (HDPA Opinion 1/2020.)

When an employer relies on the employee's explicit consent as the legal basis for processing, factors for determining whether consent was freely given include:

- The employee's dependence, as set out in the employment contract.
- The circumstances under which the employee gave consent.

(Article 27(2), Data Protection Law.)

Consent may be written or electronic and must be clearly distinguishable from the employment contract. The employer must inform the employee, in writing or electronically, about the processing purpose and the right to withdraw consent under GDPR Article 7(3). (Article 27(2), Data Protection Law.)

Controllers must take all appropriate measures to ensure they apply GDPR Article 5 principles when processing personal data in the employment context (Article 27(5), Data Protection Law; see Practice Note, Overview of EU General Data Protection Regulation: Data protection principles).

For information on workplace surveillance, see Question 31.

Cross-Border Transfer Limitations

24. **(Article 49(5), GDPR)** Does the law address or limit 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?

No. The Greek Data Protection Law does not address GDPR Article 49(5).

Complaints on Behalf of Data Subjects

25. **(Article 80(2), GDPR)** Does the law permit a body, organization, or association to lodge a complaint with the supervisory authority, independent of a data subject's mandate?

No. The Greek Data Protection Law does not include a provision permitting organizations to independently lodge complaints.

Processing Necessary to Comply with Legal Obligations or Public Interest Purposes

26. **(Articles 6(2) and 6(3), GDPR)** Does the law introduce more specific rules when processing is necessary to comply with a legal obligation under GDPR Article 6(1)(c) or necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the controller under GDPR Article 6(1)(e)?

Yes. The Greek Data Protection Law permits public bodies to process personal data where necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 5, Data Protection Law). However, according to the Hellenic Data Protection Authority, this provision is unnecessary because GDPR Article 6(1)(e) already permits this type of processing (HDPA Opinion 1/2020).

Supervisory Authorities and Fines

27. **(Article 54, GDPR)** Does the law provide for the establishment, structure, and organization of a supervisory authority?

Yes. The Greek Data Protection Law established the Hellenic Data Protection Authority (HDPA) as the supervisory authority and provides for its organization and operation (Articles 9 to 20, Data Protection Law). The HDPA has the tasks and powers specified in GDPR Articles 55 to 59.

28. **(Article 58, GDPR)** Does the law empower the supervisory authority beyond what the GDPR provides? If so, please describe those additional powers.

Yes. The Greek Data Protection Law Articles 13 to 15 assign the Hellenic Data Protection Authority with additional tasks and powers (for more, see Practice note, Greek Implementation of the GDPR: Supervisory Authority).

29. **(Article 83(7), GDPR)** Does the law provide any rules on whether and to what extent the supervisory authority may impose administrative fines on public authorities and bodies?

Yes. The Greek Data Protection Law 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 should consider when assessing administrative penalties against public bodies. The Data Protection Law does not further address administrative fines for private bodies.

30. **(Article 84, GDPR)** Does the law specify penalties for violations that are not already subject to administrative fines under Article 83?

Yes. The Greek 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).

The Hellenic Data Protection Authority has issued several enforcement decisions (in Greek). For more on key Greek enforcement actions relating to GDPR violations, see GDPR Enforcement Tracker by Country (EEA): Greece.

Video Surveillance

31. Does the law address the use of video surveillance?

Yes. Employers operating in Greece may only process personal data in the workplace through visual recording systems if:

- The processing is necessary to protect persons or goods.
- They have informed the employees in writing or electronically that a visual recording system is installed and operating in the workplace.

(Article 27(7), Greek Data Protection Law.)

Employers cannot use data collected through visual recording systems to assess employees' performance. (Article 27(7), Data Protection Law.)

Contributor profile

Tania Patsalia, Senior Associate

Bernitsas Law Firm
T +30210 3615395
E tpatsalia@bernitsaslaw.com
W www.bernitsaslaw.com/

Areas of practice: Intellectual Property, Data Protection & Privacy.

Vangelis Kalogiannis, Junior Associate

Bernitsas Law Firm
T +30210 3615395
E vkalogiannis@bernitsaslaw.com
W www.bernitsaslaw.com/

Areas of practice: Intellectual Property, Data Protection & Privacy.

END OF DOCUMENT

