Greek Implementation of the GDPR

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

Practice notes | Law stated as of 01-Jun-2021 | European Union, Greece

A Practice Note discussing the requirements of Greece's Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data, which implements the EU General Data Protection Regulation (GDPR). This Note discusses the applicability of the Greek data protection law and key provisions of the law, such as data protection officer requirements, rules for processing special categories of personal data and criminal conviction or offense data, the age of child consent, limitations on the scope of data subjects' rights, data processing for journalistic purposes or academic, artistic, or literary expression, processing for archiving in the public interest, scientific or historical research, or statistical purposes, and personal data processing in the employment context.

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) took effect on May 25, 2018, replacing the EU Data Protection Directive (Directive 95/46/EC). The GDPR introduced a single legal framework across the EU. However, the GDPR includes several provisions allowing EU member states to enact national legislation specifying, restricting, or expanding 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 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 (all 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.

This Note discusses the applicability of Greek data protection law and key Data Protection Law provisions, including requirements on:

- Appointing a data protection officer.
- Processing special categories of personal data, including genetic, biometric, and health data.
- Processing criminal conviction or offense data.
- The age of child consent.
- Limiting the scope of data subject rights and controllers' and processors' related obligations.

- Processing personal data for:
    - journalistic purposes or academic, artistic, or literary expression;
    - archiving in the public interest; and
    - scientific or historical research purposes or statistical purposes.

- Secrecy obligations.
- Processing in the employment context.
- Penalties for GDPR violations.

For more on the GDPR's application in Greece and guidance from the HDPA, see GDPR Data Protection Authority Guidance Tracker by Country (EEA): Greece.

Applicability of the GDPR and Greek Law

The GDPR applies to:

- Controllers and processors that process personal data in the context of the activities of an EU establishment, regardless of whether the data processing takes place in the EU (Article 3(1), GDPR).
- Controllers and processors not established in the EU that process personal data about data subjects in the EU when the processing activities relate to:
    - offering goods or services to data subjects in the EU, regardless of whether the controller or processor requires payment; or
    - monitoring data subjects' behavior that takes place in the EU.

    (Article 3(2), GDPR.)
- Controllers not established in the EU that process personal data and that are subject to EU member state law under public international law (Article 3(3), GDPR).

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 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).

For more on the GDPR's applicability and scope, see Practice Note, Determining the Applicability of the GDPR.

Data Protection Officers

The GDPR requires controllers and processors to appoint a data protection officer (DPO) under certain circumstances (Article 37(1), GDPR). The GDPR allows EU member states to require DPO appointments in additional situations (Article 37(4), GDPR). The Data Protection Law includes provisions on the appointment of DPOs in public bodies (Articles 6 to 8, Data Protection Law).

Public body 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.)

For more on appointing DPOs under the GDPR, see Practice Note, Overview of EU General Data Protection Regulation: Appointment of a data protection officer and GDPR Data Protection Authority Guidance Tracker by Country (EEA): Greece.

Processing Special Categories of Personal Data

The GDPR prohibits processing special categories of personal data unless an exception applies (Article 9(1), GDPR). Special categories of personal data include:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data.
- Data concerning health or sex life.
- Sexual orientation.

(Article 9(1), GDPR.)

GDPR Exceptions Permitting Processing

GDPR Article 9(2) includes several exceptions to the prohibition on processing special categories of personal data. Some of these exceptions require data controllers to consult EU or member state law to determine a lawful basis for processing.

The exceptions requiring a basis in EU or member state law include when the processing is necessary for:

- Carrying out the controller's obligations and exercising the controller's or data subjects' rights in the fields of employment law, social security, and social protection (Article 9(2)(b), GDPR).
- Reasons of substantial public interest (Article 9(2)(g), GDPR).
- Purposes of preventive or occupational medicine, assessing a data subject's working capacity, medical diagnosis, the provision of health or social care or treatment, the management of health or social care systems and services, based on EU or member state law or under a contract with a health care professional, subject to certain conditions and safeguards (Article 9(2)(h), GDPR).
- Reasons of public interest in the area of public health (Article 9(2)(i), GDPR).
- Archiving in the public interest, scientific or historical research purposes, or statistical purposes (Article 9(2)(j), GDPR).

Other GDPR Article 9 exceptions provide a sufficient legal basis for processing special categories of personal data without the need for a further basis in EU or member state law, including when the data subject consents to processing (Article 9(2)(a), (c) to (f), GDPR).

EU or member state law may prohibit the use of data subject consent as a legal basis for processing special categories of personal data (Article 9(2)(a), GDPR). However, the Data Protection Law does not prohibit this.

For more on processing special categories of personal data under the GDPR, see Practice Note, Overview of EU General Data Protection Regulation: Special categories of personal data.

Greek Law Exceptions That Permit Processing Special Categories of Personal Data

The 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 Processing in the Employment Context).

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 DPO.

(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 Processing for Secondary Purposes).
- Freedom of expression and information (Article 28, Data Protection Law; see Processing for Journalistic Purposes and Academic, Artistic, or Literary Expression).
- Archiving in the public interest (Article 29(1), Data Protection Law; see Processing for Archiving in the Public Interest).
- Scientific or historical research or statistical purposes (Article 30(1), Data Protection Law, see Processing for Scientific or Historical Research Purposes or Statistical Purposes).

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 collecting and processing genetic data for health and life insurance purposes (Article 23, Data Protection Law). According to the HDPA, any prohibition on processing genetic data extends to processing in the employment context (HDPA Opinion 1/2020; see Processing in the Employment Context).

Processing Criminal Conviction and Offense Data

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

- Carried out under the control of official authority, for example, the police.
- Authorized by EU or member state law providing for appropriate safeguards for data subjects.

(Article 10, GDPR.)

The 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 to ensure freedom of expression and the right to information.
- Consider the data subject's right to private and family life.

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

Processing for Secondary Purposes

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 member state law, which is a necessary and proportionate measure to safeguard certain important objectives, permits the processing for a secondary purpose (see GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights).

(Article 6(4), GDPR.)

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

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

(Article 6(4), GDPR.)

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 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 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 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 (see GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights). 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 GDPR Exceptions Permitting Processing and Greek Law Exceptions That Permit Processing Special Categories of Personal Data).

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

Child Consent

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, provided 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). Otherwise, it 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

The GDPR grants data subjects several rights and imposes several obligations on controllers and processors relating to those rights in Articles 12 to 22, 34, and 5 (as it relates to the rights and obligations in Articles 12 to 22) (see Practice Note, Data Subject Rights Under the GDPR). The GDPR permits EU member states to restrict the scope of these data subject rights and controllers' and processors' related obligations when the restriction is a necessary and proportionate measure to safeguard certain objectives or in specific processing situations (Articles 23 and 85 to 91, GDPR; see GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights and Derogations for Specific Processing Situations).

GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights

EU member states may restrict the scope of data subjects' rights and controllers' and processors' 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 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 claims.

(Article 23(1), GDPR.)

EU or member state laws restricting data subjects' rights to ensure GDPR Article 23 objectives should, when relevant, include provisions on:

- Purposes of the processing or categories of processing.
- Categories of personal data.
- Scope of the restrictions.
- Safeguards to prevent abuse or unlawful access or transfer.
- Specification of the controller or categories of controllers.
- Data retention periods and applicable safeguards, considering the nature, scope, and purposes of processing or categories of processing.
- Risks to data subjects' rights and freedoms.
- Data subjects' rights to be informed about the restriction unless doing so is prejudicial to the restriction's purpose.

(Article 23(2), GDPR.)

Data Protection Law Variations to Data Subject Rights

The Data Protection Law varies the following data subject rights or related controller or processor obligations when necessary to safeguard GDPR Article 23 Objectives (see GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights):

- Information rights (see Information Right).
- Access rights (see Access Right).
- Erasure rights (see Erasure Right).
- Rectification rights (see Rectification Right).
- Processing restriction rights (see Processing Restriction Right).

- Data portability rights (see Data Portability Right).
- Objection rights (see Objection Right).
- Data breach notification rights (see Data Breach Notification Right).

The 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 of 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).

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).

- 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).
- 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.)
- 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.)

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).
- 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.)

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).
- 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).

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).
- 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).

- 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).

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).
- 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).

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).
- 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).
- 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).
- 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.)

Data Breach Notification Right

The GDPR requires controllers to notify data subjects and the relevant supervisory authority of certain personal data breaches (Articles 33 and 34, GDPR). The 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).

Derogations for Specific Processing Situations

GDPR Articles 85 to 91 provide additional rules that apply to seven specific processing situations. These Articles permit EU member states to enact further rules that apply to the specified processing types. The Data Protection Law introduces further rules that apply to:

- Processing for journalistic purposes and academic, artistic, or literary expression (see Processing for Journalistic Purposes and Academic, Artistic, or Literary Expression).
- 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).
- Secrecy obligations (see Secrecy Obligations).
- Processing in the employment context (see Processing in the Employment Context).

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

The GDPR permits EU member states to establish derogations from the GDPR when necessary to reconcile the right to personal data protection with the right to freedom of expression and information, including when processing for journalistic purposes or for academic, artistic, or literary expression (Article 85, GDPR).

The 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 Data Protection Law Variations to Data Subject Rights).

Processing for Archiving in the Public Interest

The GDPR permits EU member states to establish rules when processing personal data for archiving in the public interest (Article 89, GDPR).

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 Greek Law Exceptions That Permit Processing Special Categories of Personal Data.)

Processing for archiving in the public interest may affect several data subject rights (Article 29(2) to (4), Data Protection Law; see Data Protection Law Variations to Data Subject Rights).

Processing for Scientific or Historical Research Purposes or Statistical Purposes

The GDPR permits EU member states to establish rules when processing personal data for scientific or historical research purposes or statistical purposes (Article 89, GDPR).

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 Greek Law Exceptions That Permit Processing Special Categories of Personal Data).

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 Data Protection Law Variations to Data Subject Rights).

Secrecy Obligations

The GDPR permits EU member states to adopt rules specifying the powers of supervisory authorities regarding controllers and processors that are subject to:

- An obligation of professional secrecy.
- Another equivalent secrecy obligation.

(Article 90, GDPR.)

The Data Protection Law grants the 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 in the Employment Context

The GDPR permits EU member states, by law or collective agreements, to provide more specific rules on processing personal data in the employment context (Article 88, GDPR).

The 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 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 HDPA and Opinion 1/2020; see Processing in the Employment Context).

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 relying on employee consent under the GDPR, see Practice Note, Employee Consent Under the GDPR.

Workplace Surveillance

Employers 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), Data Protection Law.)

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

Other GDPR Derogations

Processing Necessary for a Legal Obligation, Public Interest Purpose, or the Exercise of Official Authority

The GDPR permits EU member states to introduce more specific rules for processing necessary to:

- Comply with a legal obligation (Article 6(1)(c), GDPR).
- Perform a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e), GDPR).

(Article 6(2), (3), GDPR.)

Data Protection Law Article 5 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. However, according to the HDPA, this provision is unnecessary because GDPR Article 6(1)(e) already permits this type of processing (HDPA Opinion 1/2020).

Supervisory Authority

GDPR Article 54 requires each EU member state to establish a supervisory authority. The 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. The Data Protection Law assigns the HDPA with additional tasks and powers specified in Data Protection Law Articles 13 to 15.

In addition to its tasks under GDPR Article 57, the HDPA:

- 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 of the exercise of 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.)

Administrative Fines for Public Authorities and Bodies

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

Criminal Penalties for GDPR Violations

The GDPR permits EU member states to specify penalties for GDPR violations that are not subject to administrative fines under GDPR Article 83 (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).

The HDPA 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.

Data Protection Law and GDPR Statutory References

Subject Matter	Data Protection Law	GDPR Articles Permitting Member State Derogation
Applicability of the Greek law (see Applicability of the GDPR and Greek Law)	3	
Appointing a data protection officer (see Data Protection Officers)	6 to 8	37(4) and 38(5)
Processing special categories of personal data (see Greek Law Exceptions That Permit Processing Special Categories of Personal Data)	22	9(2)
Processing genetic, biometric, and health data (see Genetic, Biometric, and Health Data)	23	9(4)
Processing criminal conviction and offense data (see Processing Criminal Conviction and Offense Data)	28	10
Processing for secondary purposes (see Processing for Secondary Purposes)	24, 25	6(4)
Age of child consent (see Child Consent)	21	8(1)
Limitations on data subject rights (see Data Subjects' Rights and Data Protection Law Variations to Data Subject Rights)	31 to 35	23, 85 to 91
Processing for journalistic purposes and academic, artistic, or literary expression (see Processing for Journalistic Purposes and Academic, Artistic, or Literary Expression)	28	85
Processing for archiving in the public interest (see Processing for Archiving in the Public Interest)	29	89(3)
Processing for scientific or historical research purposes or statistical purposes (see Processing for Scientific or Historical Research Purposes or Statistical Purposes)	30	89(2)
Secrecy obligations (see Secrecy Obligations)	16	90(1)
Processing employee personal data (see Processing in the Employment Context)	27	9(4) and 88
Processing necessary for a legal obligation, public interest purpose, or the exercise of official authority (see Processing Necessary for a Legal Obligation, Public Interest Purpose, or the Exercise of Official Authority)	5	6
Supervisory authority (see Supervisory Authority)	9 to 20	51 and 54

Administrative fines for public authorities and bodies (see Administrative Fines for Public Authorities and Bodies)	39	83(7)
Criminal penalties for GDPR violations (see Criminal Penalties for GDPR Violations)	38	84

END OF DOCUMENT