Legal 500
Country Comparative Guides 2026

Greece

Data Protection & Cybersecurity

Contributor

Andersen Legal –
Pistiolis –
Triantafyllos &
Associates Law Firm

Dr. Themistoklis Giannakopoulos

Partner, Head of TMT & Data | themistoklis.giannakopoulos@gr.andersenlegal.com

Nicholas Zelios

Director | nikos.zelios@gr.andersenlegal.com

Olga Fakiola

Senior Associate | olga.fakiola@gr.andersenlegal.com

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Greece.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Greece: Data Protection & Cybersecurity

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered; what sectors, activities or data do they regulate; and who enforces the relevant laws).

The legal framework governing privacy in Greece is as follows:

- Article 9A of the Constitution which is the first constitutional text recognizing explicitly the right of individuals to the protection of their personal data and providing explicitly for the function of an independent authority entrusted with an audit role,
- The General Data Protection Regulation 2016/679 (hereinafter, 'GDPR'),
- Law No 4624/2019 which is the new Greek law that sets out implementing measures for the General Data Protection Regulation at national level,
- Law No 2472/1997 on the protection of individuals with regard to the processing of personal data, which implemented into the Greek legal order the Directive 95/46 /EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter, 'Directive 95/46/EC'),
- Law No 3471/2006 on the protection of personal data and privacy in electronic communications amending Law 2472/1997, implementing Directive 2002/58/EC on privacy and electronic communications, (hereinafter, 'Directive 2002/58/EC'),
- Law No. 5169/2025, which ratified the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (known as Convention 108+), improving safeguards in relation to data processing and new technologies.

It is noted that, pursuant to Article 84 of Law 4624/2019, a significant number of provisions of Law 2472/1997 are repealed while its provisions referred to in that article are retained.

Law 3471/2006 also remains valid and applies as lex specialis in relation to the GDPR on certain matters.

In 2020, the Hellenic Data Protection Authority (HDPA) issued an opinion on Law 4624/2019, expressing serious concerns about the compatibility of its provisions with the GDPR, while expressly stating that, in the exercise of its powers, it will not apply, provisions of Law 4624/2019 which are deemed to be in conflict with the GDPR, or are outside the authorization framework laid down by the GDPR.

With regard to the legal framework governing cybersecurity in Greece, the following are in force:

- Law 5160/2024 incorporating into Greek legislation Directive (EU) 2022/2555 ("NIS2") of the European Parliament and of the Council of 14 December 2022 concerning measures to achieve a high common level of cybersecurity across the Union, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 ("NIS");
- Law 5099/2024 on adoption of measures for the implementation of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the single market for digital services ("Digital Services Act" or "DSA"); The National Telecommunications and Post Commission (EETT) is the National Digital Services Coordinator and is responsible for supervising and checking compliance with the rules of the DSA in Greece and the Hellenic Data Protection Authority (HDPA) has been designated as competent authority for the supervision of intermediary service providers and the enforcement of point d of paragraph 1 & paragraph 3 of article 26 of the DSA (on advertising on online platforms) and Article 28 of the DSA (on online protection of minors).
- Law 5086/2024 on the establishment of National Cybersecurity Authority.
- Law No 4961/2022 on emerging information and communication technologies and strengthening digital governance, aiming to regulate the relevant issues in the public sector, including specific obligations relating to the use of Internet of Things (IoT) devices,

such as security requirements and internal record-keeping obligations.
- Law No 5002/2022 on waiving the confidentiality of communications, cybersecurity and protection of citizens' personal data.
- Law No 5193/2025, which implements aspects of the Digital Operational Resilience Act (DORA) (Regulation (EU) 2022/2554), applicable from January 2025, which is relevant to financial technology and data protection efforts in Greece, and may have implications for entities acting as ICT providers to financial institutions.
- In addition, the cybersecurity and digital regulatory framework has been further enhanced by more recent legislative developments. In particular, Law 5236/2025**,** which transposes the Critical Entities Resilience (CER) Directive, introduces a framework for the identification and supervision of critical entities across key sectors, thereby complementing and effectively expanding the scope of entities subject to cybersecurity obligations.
- Furthermore, Law 5188/2025 establishes a national framework for data governance, implementing aspects of the EU Data Governance Act and regulating data-sharing mechanisms and intermediary services.
- At EU level, the regulatory landscape continues to evolve with the introduction of the Cyber Resilience Act (CRA), which sets horizontal cybersecurity requirements for products with digital elements, while the recently adopted National Cybersecurity Strategy 2026–2030 sets out the strategic priorities for strengthening cybersecurity governance, resilience and preparedness at national level.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2026 - 2027 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments)?

On the data protection front, the HDPA is expected to intensify its enforcement activity, with a particular focus on transparency obligations, the use of AI and surveillance technologies by public authorities, and compliance with the DSA. At EU level, Greek organizations should also monitor the European Commission's Digital Omnibus Package, which proposes targeted amendments to the GDPR, and the progressive application of AI Act obligations throughout 2026, both of which will have direct practical implications for entities operating in Greece.

With regard to cybersecurity, one of the most significant developments in Greece for 2026 is the launch of the National Cybersecurity Strategy 2026–2030. The Strategy is structured around five pillars: resilient critical services, modern governance, skills development, European and international cooperation, and practical solutions.

3. Are there any identifiable trends or regulatory priorities in privacy, data protection and/or cybersecurity-related enforcement activity in your jurisdiction?

Enforcement activity in Greece shows a consistent focus on transparency, online compliance and digital marketing practices. The Hellenic Data Protection Authority has carried out repeated audits of organisations across sectors, including financial services, e-commerce and the public sector, with particular emphasis on privacy notices, cookie practices, newsletter mechanisms and website security.

A key priority is the effective exercise of data subject rights, especially the right of access and the right to erasure. Recent enforcement activity indicates increased scrutiny where organisations fail to respond adequately to such requests, including in the employment context.

There is also a growing focus on data breaches and security-related failures, as well as broader compliance obligations, such as cooperation with the authority and the proper designation and functioning of Data Protection Officers. Another identifiable trend is the increased attention to public sector processing, including the use of cloud services and broader compliance of public bodies, often in the context of coordinated actions at EU level. In addition, enforcement activity has addressed unsolicited communications and direct marketing practices, including cases involving political communications.

From a cybersecurity perspective, the focus is shifting towards the implementation and active enforcement of the NIS2 framework under Law 5160/2024, which significantly expands the scope of regulated entities and introduces stricter requirements in relation to risk management, incident reporting and governance. In practice, this is accompanied by increased regulatory scrutiny and a move towards ongoing supervision rather than purely formal compliance.

At the same time, the evolving threat landscape, including the rise of more sophisticated cyber-attacks, is driving increased regulatory attention on technical and organisational measures, supply chain risks and overall cybersecurity readiness, particularly in critical sectors and digital infrastructure.

There is also a growing emphasis on governance and management accountability, with organisations expected to demonstrate clear internal structures, policies and oversight mechanisms in relation to data protection and cybersecurity.

Overall, enforcement trends point towards a more proactive, risk-based and accountability-driven approach, with increasing emphasis on the practical implementation of compliance measures and organisational resilience.

4. Are there any registration or licensing requirements for entities covered by these data protection and cybersecurity laws, and if so what are the requirements? Are there any exemptions? What are the implications of failing to register / obtain a licence?

Under the current legal framework in Greece, there are no general registration or licensing requirements for personal data processing activities, following the direct applicability of the GDPR. The notification and prior authorisation obligations that existed under the previous regime (Law 2472/1997), including licensing requirements for the processing of sensitive personal data, have been abolished.

However, certain limited formalities remain. In particular, entities required to appoint a Data Protection Officer (DPO) pursuant to Article 37 GDPR must notify the appointment to the Hellenic Data Protection Authority.

From a cybersecurity perspective, registration obligations arise under Law 5160/2024. Entities falling within its scope must carry out a self-assessment to determine whether they qualify as “essential” or “important” entities and, where applicable, must register with the National Cybersecurity Authority (NCSA). This includes a wide range of operators across critical sectors and digital service providers, which are required to submit information regarding their activities and cybersecurity measures. Certain exemptions may apply under the cybersecurity framework, particularly in relation to entities engaged in national security, defence, public order or law enforcement activities, as well as specific public sector-related services, subject to applicable conditions.

Failure to comply with applicable requirements may lead to significant administrative fines and corrective measures. In particular, infringements of the GDPR may result in fines of up to EUR 20 million or 4% of the undertaking's global annual turnover, whichever is higher, as well as orders to suspend or restrict processing. Similarly, failure to comply with cybersecurity obligations, including registration requirements under Law 5160/2024, may trigger administrative sanctions, supervisory measures and potential operational restrictions imposed by the competent authorities.

In practice, the regulatory approach is based on an accountability model, with increased enforcement activity and a growing focus on effective implementation of compliance measures rather than formal prior authorisations.

Additional sector-specific obligations may arise under laws such as Law 4961/2022, including requirements relating to IoT security and internal record-keeping.

5. What does “personal data,” “personal information” or other equivalent terms (hereafter “personal data”) mean under data protection laws in your jurisdiction? Does the definition broadly include information about all individuals? For example, would this include individuals acting in a personal or household capacity, as well as those acting in a business or commercial capacity (such as on behalf of a business or corporate entity or employer) or otherwise?

Under the GDPR, “personal data” is defined as any information relating to an identified or identifiable natural person (“data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to identifiers such as a name, identification number, location data, online identifier or to factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

The definition is broad in scope and covers any information that can be linked to a natural person, regardless of the context in which such person is acting. This includes individuals acting both in a personal or household capacity and in a professional or business capacity, such as employees, company representatives or other individuals acting on behalf of a legal entity.

In addition, the GDPR recognises "special categories of personal data" (sensitive data), including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic, biometric and health data.

It is noted that the GDPR does not apply to the processing of personal data by a natural person during a purely personal or household activity, which constitutes a limited exemption from its scope.

6. Are certain types of personal data considered more sensitive or highly regulated under data protection laws in your jurisdiction? Please include the relevant defined terms for such data (e.g., special categories of personal data," "sensitive data" or "sensitive personal information"?

Under the GDPR, Article 9 identifies specific categories of personal data as warranting heightened protection, referred to as "special categories of personal data." These are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation. The processing of such data is prohibited in principle, subject to a limited set of exceptions exhaustively listed in Article 9(2) of the GDPR, such as explicit consent of the data subject, processing necessary for the purposes of carrying out obligations in the field of employment and social security law, or processing necessary for reasons of substantial public interest.

In addition, Article 10 of the GDPR provides for the heightened regulation of personal data relating to criminal convictions and offences.

The HDPA has consistently treated violations involving special categories of personal data as aggravating factors in the context of administrative fine calculations, resulting in higher sanctions. Organisations processing such data in Greece are expected to conduct a Data Protection Impact Assessment (DPIA) where the processing is likely to result in a high risk to the rights and freedoms of natural persons, as required under Article 35 of the GDPR.

7. What principles apply to the processing of personal data in your jurisdiction? For example: is it necessary to establish a "legal basis" for processing personal data?; are there specific transparency requirements?; must personal data only be kept for a certain period? Please provide details of such principles.

Principles relating to processing personal data are provided in article 5 of the GDPR and concern:

- lawfulness, fairness and transparency,
- purpose limitation,
- data minimization,
- accuracy,
- storage limitation, and
- integrity and confidentiality

Another principle which should be also mentioned concerns accountability, which refers to the explicit liability of the controller to demonstrate compliance with all the aforementioned principles.

In order to comply with the principle of lawfulness, processing activities must be based on one of the legal bases under article 6 referring to personal data or article 9 referring to sensitive personal data of the GDPR.

Controllers are further required to use clear and plain language in their data protection notices, as vague or ambiguous terminology, such as the use of the word "may" in describing processing activities, has been found by the HDPA to violate the transparency principle.

Moreover, the HDPA adopted, before the entry into force of the GDPR, certain regulatory acts, directives, opinions and decisions in order to regulate specific personal data processing across various business sectors. The directives and opinions serve as interpretational guidance of the existing legal framework, further specifying certain provisions. The most important among these are the following:

- Regulatory Act No 1/1999 on the obligation of the controllers to inform the data subjects,
- Directive No 115/2001 on the processing of personal data of employees,
- Directive No 1/2005 on the safe destruction of personal data,
- Directive No 1/2011 on the use of CCTV systems for the protection of persons and goods,
- Directive No 2/2011 on electronic consent,
- Opinion No 6/2013 on the access of third

parties to public documents containing personal data,
- Opinion No 1/2016 on the terms and conditions of 'opt-out' of unwanted communication for direct marketing or for other advertising purposes.

Furthermore, under Law 4624/2019 provides more specific arrangements regarding the processing of personal data:

- in the context of employment relations (Article 27),
- freedom of expression and information (Article 28),
- for archiving purposes in the public interest (Article 29),
- for the purposes of scientific or historical research or the collection and maintenance of statistics (Article 30).

However, it should be noted that the HDPA in its opinion on Law 4624/2019 has expressed considerable doubts about the compatibility of these provisions with the GDPR.

8. Are there any circumstances for which consent is required or typically obtained in connection with the processing of personal data? What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

According to the GDPR, consent is required in the following cases:

A) When there is processing of special categories of personal data. In such a case, consent is used as one of the legal bases that justifies the processing of the aforementioned categories of personal data.

B) When there is transfer of personal data to a non-EU country for which there is no adequacy decision under article 45 (3) or appropriate safeguards under article 46, including Binding Corporate Rules (hereinafter, 'BCRs'). In such a case, consent is used as one of the appropriate legal bases of data transfer.

With the newly aforementioned Greek Law no. 4624/2019, children's consent is also required for the processing of their personal data in relation to the provision of information society services directly to them, when they have reached the age of 15. If the minors are less that 15 years old, the processing referred above shall be lawful only after the consent of their legal representatives have been given.

Moreover, an indicative example where consent is required is Law 3471/2006 which prohibits unwanted communication with the data subject by electronic means, without human intervention, for purposes of direct marketing of products or services or for any other advertising purposes, unless the data subject has given his/her consent to this respect.

Another indicative example where consent is required is the example of potential borrowers, who have to give their consent to the bank in order for the latter to have access to the ''white list'' of the data system ''Tiresias'', including loans, credit cards etc.

Lastly, consent cannot be implied or obtained through silence, pre-ticked boxes, or inactivity. It must be given through a clear affirmative action. Consent should not be bundled with other terms (such as general terms of service) in a way that makes it difficult for the individual to understand what they are consenting to. Additionally, consent for multiple processing operations must be specific — separate consent must be obtained for different purposes unless they are clearly related.

9. What special requirements, if any, are required for processing particular categories of personal data (e.g., health data, children's data, special category or sensitive personal data, etc.)? Are there any prohibitions on specific categories of personal data that may be collected, disclosed, or otherwise processed?

Under the GDPR, the processing of special categories of personal data (sensitive data), such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic, biometric and health data, is in principle prohibited pursuant to Article 9(1).

However, this prohibition is lifted where one of the specific conditions set out in Article 9(2) GDPR applies. These include, inter alia, the explicit consent of the data subject, the necessity of processing for employment and social security purposes, the protection of vital interests, the establishment, exercise or defence of legal claims, reasons of substantial public interest, as well as

purposes relating to healthcare, public health, or scientific and statistical research.

In addition, national law introduces certain specific requirements. Law 4624/2019 provides for the obligation to implement appropriate and specific safeguards when processing special categories of data, particularly health data, in order to protect the rights and interests of data subjects.

Furthermore, Greek law introduces specific restrictions in certain cases. Notably, the processing of genetic data for health and life insurance purposes is generally prohibited under Article 23 of Law 4624/2019.

With regard to health data, Law 4624/2019 further specifies that processing is permitted under certain conditions, including for healthcare provision, occupational health, social protection and public health purposes, provided that appropriate safeguards and confidentiality obligations are respected.

Overall, the legal framework follows a strict prohibition-with-exceptions approach, combined with enhanced safeguards and, in certain cases, additional national restrictions.

10. Do the data protection laws in your jurisdiction have special or particular requirements, restriction, or rules regarding the collection, use, disclosure or processing of personal information from or about children or minors? If so, what is the age threshold and key requirements/restrictions that go beyond those applicable, generally?

Under the GDPR, Article 8 provides specific rules regarding the processing of personal data of children in the context of information society services offered directly to a child. Where a child is below the age of 16, such processing is lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility. Member States may legislate for a lower age threshold, provided it is not below 13 years of age.

Greece has exercised this option: Article 21 of Law 4624/2019 lowers the age threshold to 15 years, meaning that children aged 15 and above may validly consent to the processing of their personal data in the context of information society services without parental authorisation, while for children below the age of 15, consent must be given or authorised by the holder of parental responsibility.

Beyond the consent threshold, controllers offering services directly to children are required to make reasonable efforts to verify that consent has been given or authorised by the holder of parental responsibility, taking into account available technology. Privacy notices and information provided to children must be drafted in clear and plain language that is easily accessible and understandable by a child audience. Furthermore, the processing of children's personal data is identified as a factor that is likely to result in high risk, triggering the obligation to conduct a Data Protection Impact Assessment under Article 35 of the GDPR.

11. Do the data protection laws in your jurisdiction include any derogations, exemptions, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

In addition to the derogations and limitations described above, the GDPR provides for certain general exclusions from its material scope.

In particular, the GDPR does not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of EU law;
- by Member States when carrying out activities falling within the scope of national security;
- by a natural person in the course of a purely personal or household activity; and
- by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, which are instead subject to separate legal frameworks.

Furthermore, the GDPR does not apply to anonymous data, namely information which does not relate to an identified or identifiable natural person, or data rendered anonymous in such a way that identification is no longer possible. By contrast, pseudonymised data remains within the scope of data protection laws.

At national level, Law 4624/2019 largely reflects the above exclusions and does not introduce significant additional general derogations, but rather provides for specific rules in particular contexts (e.g. public sector processing and employment-related processing).

12. Does your jurisdiction require or recommend privacy risk or impact assessments in connection

with personal data processing activities and, if so, under what circumstances? How are these assessments typically carried out?

The criteria for carrying out a DPIA are classified by the HDPA, into the following three categories that were published in the Authority's Decision No 65/2018. A non-exhaustive list of data processing relevant to the entity's concerned activities, is provided for the cases where a DPIA is deemed mandatory when at least :

– Category 1: type and purposes of processing

Relevant examples:

- Systematic evaluation, scoring, prediction, prognosis and profiling, especially of clients' aspects, such as when a Bank screens its clients on the basis of credit reference data or anti-money laundering and counter-terrorist financing or fraud data.
- Systematic processing of personal data that aims at taking automated decisions producing legal effects concerning data subjects, such as the automatic refusal of an online credit application or e-recruiting practices without any human intervention.
- Systematic processing of personal data which may prevent the data subject from exercising its rights or using a service or a contract, especially when data collected by third parties are taken into account, such as when a Bank checks its customers using a creditworthiness database to determine whether or not to grant a loan, or the subject's registering in whistleblowing schemes.
- Large scale systematic processing for monitoring, observing or controlling natural persons using data collected through video surveillance systems or through networks or by any other means over a public area, publicly accessible area or private area accessible to an unlimited number of persons.
- Systematic processing with regards to profiling for the purpose of products and services promotion, under the condition that the data are combined with data collected by third parties.
- Large scale processing of health data and public health for purposes of public interest.
- Large scale processing aiming at introducing, organizing, providing and monitoring the use of electronic governance services.

– Category 2: type of data and/or categories of data subjects

Relevant examples:

- Large-scale processing of special categories of data referred to in Article 9 par.1 and the data referred to in Article 10 of the GDPR.
- Systematic and large-scale processing of data of a particularly important or exceptional nature, such as data concerning a national identification number or other identifier of general application or an alteration in the terms and conditions for the processing and use of such data and related personal data, electronic communications data, including the content of the communications such as electronic mail, data relating to social welfare (i.e. unemployment), data included in e-readers and life logging applications, data included in devices through Internet of Things Applications.
- Systematic monitoring – where permissible – of the position/location and the content and metadata of employees' communications, with the exception of logging files for security reasons, provided that the processing is limited to the absolutely y necessary data and is specifically justified. A relevant example falling under the obligation to carry out an DPIA is the use of DLP systems. Systematic processing of employees' biometric data aiming at face recognition and employees' genetic data

– Category 3: additional characteristics and/or means of the processing

Relevant examples:

- Innovative use or application of new technologies or organizational solutions with a potentially high risk to the rights and freedoms of natural persons, such as 'smart' applications, for which user profiles are generated, health applications, AI applications or blockchain technologies including personal data.
- Matching and/or combining personal data originating from multiple sources or third parties, or for two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subjects.

- In case the processing concerns personal data that has not been obtained by the data subject and the information to be provided to data subjects pursuant to Article 14 of GDPR is not possible or would require a disproportionate effort or is likely to render impossible or seriously impair the objectives of the processing.

The listing is not exhaustive and does not waive or alter the obligation to carry out a DPIA in every case where the conditions of Article 35 par. 1 of the GDPR are met, is based on Article 35 of the GDPR and in particular on paragraphs (1) and (3) of Article 35 of the GDPR and the DPIA Guidelines (WP29), which it supplements and further specifies. Furthermore, the HDPA may review and update the aforementioned listing, either on an ordinary or extraordinary basis. The methodology used to this respect in order to carry out the assessment, may vary depending on the tool that serves as a point of reference for each Data Controller concerned.

13. Are there any specific codes of practice, or self-regulatory codes applicable in your jurisdiction regarding the processing of personal data (e.g., codes of practice for processing children's data or health data)?

Codes of conduct are provided in Article 40 of the GDPR and aim at facilitating the effective application of the GDPRF regulating the relevant obligations of controllers and processors for specific areas of activity, such as insurance sector or banking. The codes of conduct shall be drawn up by associations or other bodies representing categories of controllers of processors. It should be noted that they are optional and not mandatory, and they are submitted before the HDPA which gives an opinion on whether the code aligns with GDPR. Provided that the code is adhered to by a controller or processor, it may be used as an element to demonstrate compliance with several requirements of the GDPR. Moreover, compliance with such codes shall be taken into account when deciding the imposition of a fine upon an entity. When a draft code, amendment or extension is approved and where the code of conduct concerned does not relate to processing activities in several Member State, the HDPA shall register and publish the code.

So far, draft codes of conduct have been submitted before the HDPA in sectors such as insurance, however there is no approved version that has been published by the Authority to this respect.

14. Are organisations required to maintain any records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

Most companies/organizations are required to keep a record of processing activities, which is a requirement under article 30 of the GDPR and is used as an accountability tool. The record of processing activities is also a useful tool for properly recording and organizing the company's processing activities.

Both the data controller and the data processor are required to maintain a record of processing activities with different data for each. The mandatory elements are described in detail in article 30 par. 1 of the GDPR as regards the controllers and in article 30 par. 2 with regards to the processors.

In addition to the aforementioned elements, additional information which is considered by the controller or processor as appropriate to facilitate their compliance may be included in the record of processing activities.

Any controller or processor may choose how to maintain the record of processing activities, provided that the obligation under article 30 of the GDPR is satisfied.

Furthermore, additional documentation, such as a Data Retention Policy, a Policy and Procedure on Personal Data Breach Notification and a Appropriate Use of Information Technology Resources Policy, are necessary for businesses' compliance with the GDPR.

The maintenance of the record of processing activities is not easy. Depending on the nature and the area of expertise of a company, an internal project shall be initiated to detect and record all data flows, namely the sources of data collection, data transfer channels, recipients of personal data, etc. Next, a legal audit of the flows shall take place and the legal bases shall be identified in order to be added to the record of processing activities.

Finally, the HDPA provides indicative examples of a record of processing activities on excel format in order to assist small and medium-sized enterprises in their compliance with the GDPR.

15. Do the data protection laws in your jurisdiction specifically impose data retention

limitations? If so, please describe such requirement(s).

Several decisions of the Hellenic Data Protection Authority indicate the significance of respecting the principle of limitation of the retention period as set out in Article 5 of the GDPR.

However, even though specific data retention periods may be found in the Greek legislation, there is no explicit provision for implementation of a defined data retention policy and procedure by the data controllers.

Regarding the data disposal requirements, the Authority has issued Guidelines with recommendations for the safe disposal of personal data by data controllers. These Guidelines provide a set of technical and organizational measures to ensure the secure data disposal and destruction, such as pulping for data in paper form, data alteration for data in electronic form, etc.

It is worth noting that the Authority has imposed administrative fines on data controllers for disposing personal data in non-secure ways.

16. Under what circumstances is it required or recommended to consult with the applicable data protection regulator(s)?

Under the GDPR, prior consultation with the supervisory authority is mandatory in specific circumstances.

In particular, pursuant to Article 36 GDPR, a controller is required to consult the competent supervisory authority where a data protection impact assessment (DPIA) indicates that the intended processing would result in a high risk to the rights and freedoms of individuals in the absence of appropriate mitigating measures.

In addition, consultation may effectively arise in practice in the context of personal data breaches, particularly where the breach is likely to result in a high risk to individuals, as well as in cases where organisations are required to cooperate with the supervisory authority in the exercise of its investigative or corrective powers.

Beyond these mandatory scenarios, consultation with the supervisory authority may also be recommended as a matter of good practice, for example in cases involving novel or complex processing operations, the use of new technologies, or situations where there is legal uncertainty regarding compliance with data protection requirements.

In Greece, such consultation would take place with the Hellenic Data Protection Authority.

17. Do the data protection laws in your jurisdiction require the appointment of a data protection officer, chief information security officer, or other person responsible for data protection? If so, what are their legal responsibilities?

Although Directive 95/46/ EC (article 18) included a reference on the Data Protection Officer (hereinafter, 'DPO'), Law 2472/1997 implementing the Directive did not include relevant provisions. Law 4624/2019 only refers to the appointment of a DPO by public entities, without however justifying the reason to such limited reference, not including private sector. Details on the DPO's appointment are included, such as the DPO's professional qualifications, expertise and tasks.

The formality of a DPO's appointment before the HDPA is satisfied by an electronic submission of a specific form provided by the HDPA to this respect, unless this is forbidden for public entities for reasons of national security or confidentiality duty. According to the HDPA's Opinion on Law 4624/2019 and provided that the relevant articles implement the respective provisions of Directive 2016/680, confusion might be created as per the scope of application of the respective GDPR provisions regarding DPO appointment which equally apply on both private and public entities.

In any case, the HDPA under the light of the GDPR has repeated that the role of a DPO is advisory and not determining and that the DPO does not have personal liability for non-compliance with the requirements of the GDPR. Appointment is concluded in writing, whereas the relevant tasks and role should be framed in accordance with the GDPR's relevant provisions. Amongst the DPO's tasks the HDPA has identified raising awareness and data protection culture within the entity concerned, informing and consulting the entity as per its obligations arising from the legal framework. The DPO should also monitor internal compliance, undertake personnel's training, conduct internal audits, advise on DPIAs and follow up their implementation. Furthermore, the DPO should serve as the contact person for both supervisory authorities and data subjects and should further cooperate with the supervisory authority.

With regard to cybersecurity, Law 5160/2024, Article 15 para 5, essential and important entities must appoint a qualified executive, with appropriate training and

expertise, as the Information and Communication Systems Security Officer (Y.A.S.P.E.), who will be responsible for managing all communications and contacts with the National Cybersecurity Authority, and ensuring internal coordination for the entity's compliance with the requirements of this article, as well as incident reporting requirements as per Article 16.

The Information and Communication Systems Security Officer (Y.A.S.P.E.) shall be provided by the entity with the necessary resources to carry out their duties, which are incompatible with those of the Data Protection Officer (D.P.O.) as defined in Article 37 of Regulation (EU) 2016/679 of the European Parliament and Council. They shall have an appropriate level of decision-making autonomy, the ability to implement decisions within the various organizational units of the entity, to inform the governing bodies, to coordinate security incident management, as well as to implement business continuity and disaster recovery plans. The qualifications, duties, incompatibilities, and obligations of the Y.A.S.P.E. have been further elaborated in Ministerial Decision No. 1899/2025.

For central government entities, as defined in paragraph (c) of section 1 of Article 14 of Law 4270/2014 (A' 143), Articles 18 and 19 of Law 4961/2022 (A' 146) apply regarding the appointment, qualifications, and duties of the Information and Communication Systems Security Officer.

18. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s) or recommendation(s).

Under the GDPR and Law 4624/2019, there is no explicit statutory obligation requiring organisations to provide employee training on data protection.

However, employee training is considered a key element of compliance under the accountability principle (Article 5 GDPR), as part of the implementation of appropriate technical and organisational measures.

In practice, the Hellenic Data Protection Authority has consistently emphasised the importance of staff training through its case law. In particular, the HDPA has identified employee training as an essential organisational measure to ensure compliance and has taken into account the existence (or absence) of training programmes when assessing infringements and determining administrative fines.

As a result, while not formally required, employee training is strongly recommended and is generally expected by the supervisory authority, especially for staff involved in processing activities or handling personal data breaches.

In practice, organisations are expected to implement regular and systematic training programmes, as part of a broader compliance framework demonstrating adherence to GDPR requirements.

19. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

Under the GDPR, controllers are required to provide clear, transparent and easily accessible information to data subjects regarding the processing of their personal data, in accordance with Articles 13 and 14.

This obligation applies both where personal data is collected directly from the data subject and where it is obtained indirectly from third parties, subject to limited exceptions. The information must be provided at the time of collection (or within a reasonable period, where data is not obtained directly) and must be presented in a concise, intelligible and easily accessible form.

In terms of content, controllers are required to inform data subjects, inter alia, of their identity and contact details (and those of the data protection officer, where applicable), the purposes and legal basis of the processing, any recipients of the data, potential international transfers, the applicable retention period, and the rights available to data subjects, including the right to lodge a complaint with the supervisory authority.

In practice, these obligations are typically fulfilled through privacy notices, including website privacy policies, layered notices and just-in-time disclosures, particularly in digital environments.

At national level, Law 4624/2019 provides for certain limited derogations, primarily in cases where data is not obtained directly from the data subject, for reasons such as national security, public security or the establishment, exercise or defence of legal claims, subject to compliance with EU law.

From an enforcement perspective, the Hellenic Data Protection Authority has consistently placed emphasis on the transparency and completeness of privacy notices, particularly in online environments, including in relation

to cookies and digital services, indicating that the quality of information provided to data subjects is a key area of regulatory scrutiny.

20. Do the data protection laws in your jurisdiction distinguish between the responsibilities of "controllers" and those of "processors" (or equivalent terms) of personal data? If so, how are such terms defined and what are the key distinctions between the obligations of controllers and processors (or equivalent terms)?

It is clear from the wording of article 3 paras 1 and 2 of the GDPR that the latter applies directly to both the data controller and the data processor.

Moreover, at national level, under the previous legal regime, there was a provision in article 3 par. 3 of L. 2472/1997, for the direct applicability of relevant provisions to both the data controller and the data processor. However, under Law 4624/2019, there is no corresponding reference.

Furthermore, there are both national and GDPR provisions that, taking into consideration the nature and scope of each role, distribute specific responsibilities and distinct obligations upon the data controller and the data processor.

In addition, and in accordance with article 28 of the GDPR, a contractual relationship between the controller and the processor, the exact content of which is specified in the above article, is required and includes the details mentioned above, in the relevant question under No 13.

21. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these or any similar terms defined?

In addition to the GDPR provisions on monitoring and profiling, at national level, HDPA regulates and further interprets through its Directives specific aspects of these matters, such as Directive 115/2001 which defines monitoring at the workplace and Directive 1/2011 on CCTV monitoring. CCTV monitoring at the workplace is also regulated by article 27 of Law 4624/2019. Moreover, with regards to the use of tracking technologies such as GPS, the HDPA by a set of decisions has defined the framework of GPS operation and use by data controllers, while with regards to cookies, the provisions of Law 3471/2006 remain in force.

Article 4 par. 5 of Law 3471/2006 stipulates that installation of cookies is only allowed if the subscriber or user has given his/her consent after having been clearly and extensively informed.

Therefore, according to the above, the provider of an online service (for example an e-shop) or a third party (for example, an advertising site which promotes products through a website of an e-shop) may install cookies only if the subscriber or user has given his/her consent to this after having been duly informed (with the exception of the technically necessary cookies). To this respect the HDPA has provided guidance on good and bad practices regarding the implementation of cookies banners and the appropriate information towards the data subjects, calling the data controllers to comply with these recommendations. It is worth noted that this was also an issue that was audited when the HDPA conducted the remote ex-officio investigations across various websites.

Moreover, regarding automated decision making, Law 4961/2022 "on emerging information and communication technologies, the reinforcing of digital governance and other provisions", establishes a coherent legislative framework for artificial intelligence ("AI"). The Law stipulates that prior to the initial use of an AI system, which affects the decision-making process concerning employees, existing or prospective, and has an impact on their conditions of employment, selection, recruitment or evaluation, each entity shall provide relevant information to the employee. The relevant obligation also applies to digital platforms in respect of natural persons linked to them by employment contracts or independent service provision or project agreements. For any violation of this obligation, penalties are imposed by the Labour Inspectorate.

22. Do the laws in your jurisdiction include specific rules, requirement or regulator guidance regarding the use of cookies, pixels, online tracking and/or targeted advertising? Please describe any restrictions on targeted advertising and/or cross context behavioral advertising. How are these terms or any similar terms defined?

The use of cookies, tracking technologies and online behavioural advertising in Greece is primarily regulated under Law 3471/2006, in conjunction with the GDPR.

Under this framework, the storage of information or

access to information stored in a user's terminal equipment (including through cookies, pixels and similar tracking technologies) generally requires the prior informed consent of the user, following clear and comprehensive information.

An exception applies for cookies or trackers that are strictly necessary for the transmission of a communication or for the provision of an information society service explicitly requested by the user, which do not require consent.

Although terms such as "targeted advertising" or "behavioural advertising" are not explicitly defined in Greek legislation, they are commonly understood to refer to advertising practices based on the tracking and profiling of users' behaviour, typically through cookies and similar technologies.

In this context, targeted and cross-context behavioural advertising is subject to the same consent requirements, meaning that the use of non-essential tracking technologies for advertising or profiling purposes is not permitted without the user's prior consent.

The Hellenic Data Protection Authority has issued guidance and recommendations on the use of cookies and tracking technologies, placing particular emphasis on:

- the validity of consent (which must be freely given, specific, informed and explicit),
- the prohibition of pre-ticked boxes or implied consent, and
- the requirement for clear and user-friendly cookie banners and consent management mechanisms.

In practice, the HDPA has actively enforced these requirements, particularly in relation to online services, indicating that tracking technologies and targeted advertising practices remain an area of increased regulatory scrutiny.

23. Do the data protection laws in your jurisdiction specifically restrict or regulate the "sale" of personal data and/or "data brokers"? How is "sale" and/or "data broker" or (similar/related terms) defined?

Under the GDPR and the applicable Greek legal framework, there is no specific legal concept of "sale" of personal data or "data brokers", nor a distinct regulatory regime governing such activities as such.

Instead, any transfer, disclosure or commercial use of personal data is assessed under the general data protection principles and legal bases set out in the GDPR, including lawfulness, transparency and purpose limitation. In practice, activities commonly described as the "sale" of personal data would typically fall within the notion of processing, and must be justified on a valid legal basis, most commonly the consent of the data subject or, in limited cases, the legitimate interests of the controller, subject to the balancing test.

In addition, the use of personal data for direct marketing purposes, which may overlap with certain data monetisation practices, is subject to specific rules under Law 3471/2006, including requirements for prior consent (particularly in electronic communications).

Although the terms "sale of personal data" and "data brokers" are not defined under Greek law, they are generally understood in practice to refer to the commercial disclosure or exchange of personal data to third parties, often for marketing or profiling purposes.

From an enforcement perspective, the Hellenic Data Protection Authority has taken a strict approach to unlawful data sharing and marketing practices, indicating that any form of data commercialisation is subject to scrutiny under the GDPR framework, particularly as regards transparency, valid consent and fair processing.

24. Do the data protection laws in your jurisdiction specifically regulate or restrict marketing and electronic communications, including telemarketing/telephone solicitations and 'robocalls', email marketing, SMS/text messaging or other direct marketing? Please provide an overview.

Direct marketing and electronic communications in Greece are primarily regulated under Law 3471/2006, which implements the ePrivacy Directive, in conjunction with the GDPR.

As a general rule, the use of electronic communications for direct marketing purposes, including email, SMS and automated calling systems (e.g. robocalls), requires the prior consent of the recipient (opt-in regime).

In contrast, telephone calls with human intervention are subject to an opt-out regime, meaning that such calls are permitted unless the subscriber has previously objected, either by registering on relevant opt-out lists or directly notifying the controller.

An important exception applies to existing customer relationships (the "soft opt-in"), whereby a company may use contact details obtained in the context of a sale of goods or services to promote similar products or services, provided that:

- the contact details were lawfully obtained;
- the marketing concerns similar products or services; and
- the recipient is given a clear and easy opportunity to object, free of charge, both at the time of data collection and with each subsequent communication.

In addition, the Hellenic Data Protection Authority has issued guidance and recommendations on electronic marketing practices, including the conditions for valid consent and the proper use of the soft opt-in exemption.

Overall, the Greek framework establishes a strict consent-based regime for electronic marketing, complemented by specific rules for telephone communications and limited exceptions for existing customer relationships.

25. Do the data protection laws in your jurisdiction regulate, restrict or impose specific obligations on the processing of biometric data, such as facial recognition. If so, how are the relevant terms defined? Are these obligations focused on the collection, use and processing of unique biometric 'identifiers' (rather than any sort of biometric measurements) ?

Under the GDPR, biometric data is defined (Article 4(14)) as personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that person, such as facial images or fingerprint data.

Biometric data constitutes a special category of personal data under Article 9 GDPR, and its processing is, in principle, prohibited unless one of the specific legal bases set out in Article 9(2) applies. In Greece, Law 4624/2019 does not introduce a separate standalone regime for biometric data, but requires the implementation of appropriate safeguards when such data is processed.

In practice, the use of biometric data (including facial recognition technologies) is subject to strict scrutiny, particularly given its intrusive nature and the risks it poses to fundamental rights. The Hellenic Data Protection Authority has adopted a restrictive approach in its enforcement practice, particularly in cases involving biometric access control systems, emphasizing the need for strict necessity, proportionality and prior impact assessments.

Moreover, processing involving biometric data will, in most cases, trigger the obligation to conduct a data protection impact assessment (DPIA).

Importantly, the regulatory framework focuses on biometric data used for the purpose of uniquely identifying individuals, rather than on biometric measurements in general. As such, not all biometric-related data falls within the stricter regime, but only data processed through specific technical means enabling identification.

26. Are there any data protection laws in your jurisdiction that specifically address or apply to artificial intelligence or machine learning ("AI"). If so, do these laws specifically apply to the processing of personal information related to AI, or more broadly?

Greece enacted Law 4961/2022 in July 2022 to promote the responsible use of emerging technologies. This law covers Artificial Intelligence (AI), Internet of Things (IoT), Unmanned Aircraft Systems (UAS), Distributed Ledger Technologies (DLT), and 3D Printing. The purpose of Law 4961/2022 is the lawful, safe and secure development, deployment and use of AI technologies by public and private entities and the accommodation of the potential of IoT, UAS, DLT and 3D Printing for the public sector and the market.

In addition, at the European Union level, the EU Artificial Intelligence Act (AI Act) was adopted in 2024 and is directly applicable in Greece. The AI Act introduces a comprehensive regulatory framework for AI, based on a risk-based approach, imposing specific obligations depending on the level of risk posed by the AI system (unacceptable, high, limited or minimal risk). The AI Act sets out rules on transparency, human oversight, data governance, and conformity assessments, particularly for high-risk AI systems.

27. Are there any data localization requirements in your jurisdiction? In other words, are there any circumstances where some or all personal data is required to be stored locally, or prohibited from

being transferred to or stored in certain jurisdictions?

Under the GDPR and the applicable Greek legal framework, there are no general data localisation requirements mandating that personal data must be stored within Greece.

However, the transfer of personal data outside the European Economic Area (EEA) is subject to the restrictions set out in Chapter V of the GDPR. In particular, such transfers are permitted only where:

- the European Commission has adopted an adequacy decision for the recipient country; or
- appropriate safeguards are in place, such as standard contractual clauses (SCCs), binding corporate rules or other approved transfer mechanisms; or
- a specific derogation applies under Article 49 GDPR.

In the absence of the above conditions, transfers of personal data to third countries are prohibited.

Greek law does not generally impose additional localisation requirements beyond those established under the GDPR. However, in practice, certain sector-specific considerations (e.g. in relation to public sector data or critical infrastructure) may influence how and where data is stored or processed.

Overall, the Greek framework follows the EU approach of regulating international data transfers rather than imposing strict localisation requirements.

28. Is the transfer of personal data outside your jurisdiction restricted, under certain circumstances? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

Under the GDPR, transfers of personal data outside the European Economic Area (EEA) are restricted and can only take place under specific conditions set out in Chapter V.

In particular, such transfers are allowed where:

- the European Commission has adopted an adequacy decision for the recipient country; or
- appropriate safeguards are in place, most commonly standard contractual clauses (SCCs) or binding corporate rules (BCRs); or
- one of the limited exceptions under Article 49 GDPR applies (e.g. explicit consent or necessity for contract performance).

In practice, most organisations rely on SCCs, often combined with a transfer impact assessment and additional safeguards, depending on the circumstances of the transfer.

Generally, no prior notification or authorisation from the supervisory authority is required when relying on standard mechanisms such as SCCs. However, certain tools, such as BCRs, do require approval.

In Greece, supervision is carried out by the Hellenic Data Protection Authority, in line with the broader EU approach.

29. What personal data security obligations are imposed by the data protection laws in your jurisdiction?

The HDPA refers to the provisions of the GDPR on the obligations of the controller and the processor regarding security of processing. These obligations are explicitly defined in article 32 of the GDPR. In addition, article 24 of the GDPR provides for the overall responsibility of the controller to identify and implement appropriate technical and organizational measures. The objective of the security measures is to maintain confidentiality, integrity and availability of personal data.

The GDPR suggests 'appropriate' technical and organizational security measures such as the pseudonymization and encryption of personal data, adherence to an approved code of conduct or an approved certification mechanism to demonstrate compliance, procedures on how to handle data breach cases, etc.

Moreover, Law 4624/2019 (article 22) provides that when processing special categories of personal data, all appropriate and specific measures must be taken to safeguard the personal data subject's interests. These measures may include amongst others, in particular:

- measures to ensure that ex-post verification can be carried out and the identification of whether and by whom personal data has been entered, modified or deleted
- measures to raise employees' awareness in processing personal data

- restrictions on access by controllers and processors
- the pseudonymization of personal data
- encryption of personal data
- measures to ensure the confidentiality, integrity, availability and durability of processing systems and services related to the processing of personal data
- procedures to regularly test and evaluate the effectiveness of technical and organizational measures in order to ensure the safety of processing.

Security measures can be documented in individual procedures or in more general security policies. The determination of appropriate security measures shall be made taking into consideration the latest developments, the cost of implementation, the processing features, the scope and purposes of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

With regards to the specific security measures and the security policies and procedures that an organization must follow, it should be noted that the HDPA, in an earlier text of informative nature, suggests a code of conduct, a security policy, a security plan and/or a disaster recovery plan. Finally, the 'ex officio' investigations conducted by the HDPA on the security measures of various websites include the https protocol settings, the validity of digital certificates, the password security criteria, and so on.

30. Are there more specific security obligations for certain types of personal data (e.g., sensitive data or special categories of personal data)?

The general security obligations under Article 32 of the GDPR apply, requiring controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Where special categories of personal data are involved, the inherently higher risk associated with such data necessitates more robust security measures, and the HDPA has consistently treated inadequate security in this context as an aggravating factor in fine calculations.

In addition, where processing of special categories of personal data is likely to result in a high risk to the rights and freedoms of data subjects, controllers are required under Article 35 of the GDPR to carry out a Data Protection Impact Assessment prior to commencing the processing. The HDPA has published a list of processing operations for which a DPIA is mandatory, which includes large-scale processing of health data, biometric data processed for identification purposes, and genetic data.

In specific sectors, additional security obligations apply by virtue of Greek sectoral legislation. In the healthcare sector, relevant ministerial decisions impose further safeguards. In the electronic communications sector, Law 3471/2006 imposes specific security obligations on providers of publicly available electronic communications services. Under Law 5160/2024, essential and important entities, many of which process special categories of personal data, are required to implement appropriate technical, operational, and organisational measures to manage cybersecurity risks, which necessarily encompasses the security of any personal data processed within their systems.

31. Do the data protection laws in your jurisdiction impose obligations in the context of security breaches which impact personal data? If so, how do such laws define a security breach (or similar term) and under what circumstances and within what timeframe must such a breach be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

The HDPA, when it comes to personal data breach incidents, refers to the provisions of the GDPR and to articles 33 and 34 of the GDPR regarding the obligation to notify the breach to the supervisory authority and to communicate the breach to the data subject.

A personal data breach is defined by the GDPR as follows: a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Laws 2472/1997 and 4624/2019 do not include any provision concerning personal data breach incidents. The only exception is Law 3471/2006 which provides for a special data breach notification procedure to the HDPA and the Hellenic Authority for Communication Security and Privacy (ADAE) followed by providers of publicly available electronic communications services.

According to Law 3471/2006 a personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed in relation to the provision of publicly available electronic communications services.

32. Do the data protection laws in your jurisdiction establish specific rights for individuals, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, and any exceptions.

The GDPR establishes a comprehensive set of rights for individuals (data subjects), aimed at ensuring transparency and control over the processing of their personal data.

These include, in particular, the right to be informed, the right of access, the right to rectification, the right to erasure ("right to be forgotten"), the right to restriction of processing, the right to data portability, and the right to object to processing. In addition, individuals have the right not to be subject to decisions based solely on automated processing, including profiling, and the right to withdraw consent at any time where processing is based on consent.

These rights are typically exercised by submitting a request to the controller through accessible means (e.g. email or online forms). Controllers are required to respond without undue delay and in any event within one month, with the possibility of a two-month extension where necessary due to complexity or volume of requests. As a general rule, responses must be provided free of charge, although a reasonable fee may be charged, or the request refused, where requests are manifestly unfounded or excessive.

At national level, Law 4624/2019 provides for certain limitations and restrictions on the exercise of these rights under specific conditions, including for reasons of national security, public security, or the protection of the rights and freedoms of others. However, such restrictions must be interpreted in line with EU law requirements.

In addition, sector-specific rules may apply. For example, Law 3471/2006 provides for certain rights in the context of electronic communications (e.g. information rights in relation to call recording and traffic or location data), while the Hellenic Data Protection Authority has issued guidance on the practical exercise of rights in specific contexts, such as video surveillance.

Overall, the framework provides individuals with extensive and enforceable rights, with increasing regulatory focus on their effective implementation in practice.

33. Do the data protection laws in your jurisdiction allow or provide for a private right of action for violations? If so, does your jurisdiction also allow "class action" litigation (i.e., on behalf of a class or ('many') claimants)? Please explain under what circumstances in which a private right of action applies and/or a class action may be brought, and whether types of claims/violations present a higher risk of a private right of action or class action (e.g., are there statutory damages or presumed harm for certain violations)?

Under the GDPR, individuals have a direct right to seek judicial remedies against controllers or processors for violations of data protection law.

In particular, Article 82 GDPR provides that any person who has suffered material or non-material damage as a result of an infringement has the right to receive compensation. This includes claims for financial loss as well as moral harm (e.g. distress or reputational damage).

At national level, Law 4624/2019 further regulates judicial protection, including the competent courts and procedural aspects. In addition, individuals may challenge decisions of the Hellenic Data Protection Authority before the competent administrative courts.

Greek law also allows data subjects to mandate non-profit bodies, organisations or associations to lodge complaints and seek judicial remedies on their behalf, in line with Article 80 GDPR.

As regards collective redress, Greece does not have a US-style class action system in the data protection field. However, representative actions by associations or collective consumer claims may be brought under certain conditions, particularly where multiple individuals are affected.

Certain types of infringements, such as data breaches, unlawful disclosures or direct marketing violations, are more likely to give rise to compensation claims, especially where individuals can demonstrate harm. While there are no statutory damages or presumed compensation amounts, Greek courts recognise both material and non-material damage, which may increase litigation risk in practice.

Overall, the framework provides for individual and, to a more limited extent, collective enforcement mechanisms, with a growing focus on compensation claims following

data protection violations.

34. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual and material damage to have been sustained, or is non-material injury to feelings, emotional distress or similar sufficient for such purposes?

Under the GDPR, individuals are entitled to seek compensation for both material and non-material damage resulting from violations of data protection law.

In particular, Article 82 GDPR provides that any person who has suffered damage because of an infringement has the right to receive compensation from the controller or processor. Importantly, this includes not only financial loss, but also non-material harm, such as distress, reputational damage, or loss of control over personal data.

At national level, Law 3471/2006 further supports this approach, expressly recognising compensation for injury of feelings, independently of any financial damage. Greek case law has confirmed that such non-material harm may arise directly from the infringement itself, particularly in cases involving unsolicited communications or violations of privacy in electronic communications.

As a result, Greek law does not require proof of material damage for compensation to be awarded. Non-material damage alone may be sufficient, subject to judicial assessment in each case.

In practice, claims are more likely to arise in cases such as data breaches, unlawful disclosures or intrusive marketing practices, where individuals can demonstrate an impact on their private life or personal sphere.

35. How are data protection laws in your jurisdiction typically enforced? What regulatory body(ies) have enforcement authority?

According to articles 9 to 15 of the Greek Law 4624/2019, the HDPA is entrusted with supervisory and sanctioning powers related to the application of the rules on the protection of personal data. Additionally, the Hellenic Authority for Communication Security and Privacy (ADAE) has been established according to article 19 par. 2 of the Hellenic Constitution, with the purpose is to protect the free correspondence or communication, as well as the security of networks and information in any possible way.

36. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction? Are there any guidelines or rules for the calculation of such fines or the imposition of sanctions?

Under the GDPR, infringements of data protection law may result in a wide range of corrective powers and administrative fines imposed by the competent supervisory authority.

In particular, supervisory authorities may impose corrective measures such as warnings, reprimands, orders to comply, temporary or definitive limitations (including bans) on processing, as well as orders to rectify, erase or restrict data processing.

Administrative fines under the GDPR can reach:

- up to EUR 10 million or 2% of the total worldwide annual turnover of the preceding financial year (for certain infringements); or
- up to EUR 20 million or 4% of the total worldwide annual turnover (for more serious infringements),

whichever is higher.

In Greece, these powers are exercised by the Hellenic Data Protection Authority, which may also impose additional administrative measures under Law 4624/2019.

As regards the calculation of fines, Article 83 GDPR sets out the key criteria to be considered, including:

- the nature, gravity and duration of the infringement;
- whether the infringement was intentional or negligent;
- any action taken to mitigate damage;
- the degree of responsibility of the controller or processor;
- previous infringements;
- the level of cooperation with the supervisory authority; and
- the categories of personal data affected.

In practice, the HDPA follows the GDPR criteria and relevant European guidance, including guidance issued by the European Data Protection Board, and adopts a case-by-case approach, taking into account both aggravating

and mitigating factors.

Overall, the sanctions regime is broad and flexible, combining significant financial penalties with corrective powers aimed at ensuring compliance.

37. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

In Greece, enforcement decisions issued by the Hellenic Data Protection Authority may be challenged before the competent administrative courts.

Under Law 4624/2019, legally binding decisions of the HDPA, including those imposing administrative fines or other corrective measures, are subject to judicial review, with jurisdiction ultimately lying with the Council of State.

In addition, the GDPR (Article 78) provides for the right to an effective judicial remedy against supervisory authority decisions.

In practice, appeals typically focus on the legality of the decision, the assessment of the facts, and the proportionality of the sanction imposed.

38. Do the cybersecurity laws in your jurisdiction require the implementation of specific cybersecurity risk management measures and/or require that organisations take specific actions relating to cybersecurity? If so, please provide an overview of these obligations and explain their scope/applicability. For example, are all organizations subject to the requirement or only to certain organizations (e.g., based on size, sector, critical infrastructure designation, public company)? Are there specific and/or additional regulations for different industries (e.g., finance, healthcare, government)?.

Yes. Under Law 5160/2024, organisations falling within its scope are required to implement appropriate technical, operational and organisational measures to manage cybersecurity risks.

These obligations apply primarily to entities classified as “essential” and “important”, covering a wide range of sectors, including energy, transport, banking, health, digital infrastructure and certain digital service providers. The scope is therefore sector-based and risk-based, rather than applying to all organisations.

In particular, Article 15 of the law requires entities to adopt a comprehensive set of risk management measures, including:

- risk analysis and information security policies;
- incident detection and response procedures;
- business continuity and crisis management measures;
- basic cyber hygiene practices and staff training;
- policies on the use of cryptography and encryption; and
- secure authentication measures, including multi-factor authentication where appropriate.

In addition, entities are subject to obligations relating to incident reporting, governance and management accountability, reflecting the broader requirements of the NIS2 framework.

Further sector-specific requirements may apply in certain industries. For example, financial institutions are subject to additional obligations under the framework implementing the Digital Operational Resilience Act (DORA), while public sector bodies and critical infrastructure operators are subject to enhanced supervision.

39. Do the cybersecurity laws in your jurisdiction impose formal cybersecurity audit or certification requirements? If so, please provide an overview.

Under Law 5160/2024, there is no general obligation for entities to obtain a formal cybersecurity certification.

However, the law establishes a structured supervisory and audit framework. The National Cybersecurity Authority is empowered to carry out both ex ante and ex post supervision of entities falling within its scope, including regular and ad hoc audits, inspections and on-site visits, based on a risk-based approach. Audit activities may also be carried out by certified inspectors accredited by the Authority.

In addition, entities may be required, in practice, to use ICT products, services or processes that are certified under European cybersecurity certification schemes adopted under Regulation (EU) 2019/881 (EU Cybersecurity Act), as part of demonstrating compliance.

Overall, while there is no direct obligation for entities to obtain certification, the framework combines mandatory supervision and audits with an increasing reliance on certified technologies and standards.

40. Do the cybersecurity laws in your jurisdiction impose specific requirements regarding vendor and supply chain management? If so, please provide details of these requirements.

Yes. Under Law 5160/2024, entities falling within its scope are required to address cybersecurity risks arising from their supply chain as part of their broader risk management obligations.

In particular, Article 15 expressly refers to the security of the supply chain, including aspects relating to relationships with direct suppliers and service providers. Entities are required to take into account the vulnerabilities of their suppliers, as well as the overall quality of their cybersecurity practices, especially where such third parties support critical functions.

These obligations form part of a risk-based approach and do not establish a standalone vendor management regime but rather integrate supply chain security into the overall cybersecurity governance framework.

Additional sector-specific requirements may apply in certain industries. For example, financial entities are subject to more detailed third-party risk management obligations under the framework implementing the Digital Operational Resilience Act (DORA).

41. Do the cybersecurity laws in your jurisdiction require the appointment of a chief information security officer, regulatory point of contact, or other person responsible for cybersecurity? If so, please provide an overview of the requirement, including whether there are any formalities that must be observed regarding such appointment (e.g., board-approval, reporting line structure, notification to regulatory body).

Yes. Under Law 5160/2024, entities classified as “essential” and “important” are required to appoint an Information and Communication Systems Security Officer (I.C.S.S.O.).

Pursuant to Article 15(5), the I.C.S.S.O. acts as the primary point of contact with the National Cybersecurity Authority and is responsible for coordinating compliance with cybersecurity obligations, including incident reporting requirements. The role also includes overseeing internal implementation of cybersecurity measures and ensuring ongoing compliance with the applicable framework.

The appointed officer must be provided with the necessary resources and must have an appropriate level of autonomy in the performance of their duties, including the ability to inform senior management and coordinate incident response and business continuity processes. The role is expressly incompatible with that of the Data Protection Officer.

While the law does not provide for specific formalities such as prior regulatory approval or notification of the appointment, it establishes a structured governance requirement, ensuring that cybersecurity responsibilities are clearly assigned within the organisation.

42. Do the cybersecurity laws in your jurisdiction impose specific reporting or notice obligations in the context of cybersecurity incidents? If so, how do such laws define a cybersecurity incident and what are the reporting and notification requirements (please also note whether these laws require reporting of certain cyber security incidents, regardless of whether there has been a ‘breach of personal data’)?

Yes. Under Law 5160/2024, entities classified as “essential” and “important” are subject to specific incident reporting and notification obligations.

A cybersecurity incident is generally understood as any event compromising the availability, authenticity, integrity or confidentiality of network and information systems, with reporting obligations triggered where the incident has a significant impact on the provision of services.

In such cases, entities are required to notify the competent Computer Security Incident Response Team (CSIRT) of the National Cybersecurity Authority without undue delay. The reporting framework follows a staged approach, including:

- an early warning notification, providing an initial indication of the incident;
- a more detailed incident notification, including an assessment of its severity and potential cross-border impact; and
- a final report, outlining the root cause, mitigation measures and overall impact.

Importantly, these obligations apply to cybersecurity incidents as such and are not limited to personal data breaches.

In addition, where appropriate, entities must inform

affected service recipients of significant incidents that may adversely affect the provision of services, including relevant information on the nature of the threat and any mitigation measures.

43. Can individuals bring a private right of action for cybersecurity incidents or other violations of cybersecurity laws? If so, does your jurisdiction also allow "class action" litigation (i.e., on behalf of a class or ('many') claimants)? Please explain under what circumstances in which a private right of action and/or a class action may be brought?

Under Law 5160/2024, there is no specific private right of action for individuals affected by cybersecurity incidents, nor does the law establish a dedicated civil liability or collective redress regime. Enforcement is primarily administrative, through supervisory powers exercised by the National Cybersecurity Authority, including audits, corrective measures and administrative fines.

However, affected individuals may seek compensation under general civil law provisions, in particular tort liability under the Greek Civil Code. In addition, where a cybersecurity incident involves a personal data breach, individuals may rely on the right to compensation under GDPR (Article 82).

As regards collective redress, Greek law does not recognise US-style class actions. However, certain forms of collective or representative actions are available in limited contexts, particularly under consumer protection legislation and, in specific cases, under data protection law where organisations may act on behalf of data subjects.

44. How are cybersecurity laws in your jurisdiction typically enforced? What regulatory body(ies) have enforcement authority?

Cybersecurity laws in Greece are primarily enforced through administrative supervision by the National Cybersecurity Authority, which is the main competent authority under Law 5160/2024.

The National Cybersecurity Authority is responsible for monitoring compliance with cybersecurity obligations, maintaining the registry of "essential" and "important" entities, and exercising supervisory powers, including audits, inspections and the imposition of administrative sanctions. It also operates the national Computer Security Incident Response Team (CSIRT), which plays a central role in incident handling and coordination.

In addition, other authorities may be involved depending on the nature of the incident. Where cybersecurity incidents involve personal data, the Hellenic Data Protection Authority is competent to enforce data protection rules under the GDPR.

Further, the Hellenic Authority for Communication Security and Privacy (ADAE) has competence in relation to the confidentiality of communications, including oversight and audits of relevant providers, while cybercrime-related offences are investigated and prosecuted by the Cyber Crime Division of the Hellenic Police.

45. What powers of oversight / inspection / audit do regulators have in your jurisdiction under cybersecurity laws.

Under Law 5160/2024, the National Cybersecurity Authority is vested with extensive oversight, inspection and audit powers to monitor compliance with cybersecurity obligations.

In particular, the Authority may carry out on-site and remote inspections, with or without prior notice, and conduct investigations within the premises of regulated entities. It is empowered to request access to information, data and documentation necessary to assess compliance, including evidence relating to the implementation of cybersecurity policies and risk management measures. It may also perform targeted security audits and security scans, based on a risk-based approach.

In the case of essential entities, the supervisory framework is more stringent and includes enhanced oversight measures, such as regular and targeted audits, requests for detailed information, and continuous monitoring of risk management practices.

In addition, other authorities may exercise oversight powers depending on the nature of the incident or the sector concerned. In particular, the Hellenic Data Protection Authority may investigate and impose sanctions where cybersecurity incidents involve personal data, while the Hellenic Authority for Communication Security and Privacy has audit and inspection powers in relation to the confidentiality and security of communications. Cybercrime-related matters may also fall within the investigative powers of the Hellenic Police.

46. What is the range of sanctions (including fines and penalties) for violations of cybersecurity laws in your jurisdiction? What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction? Are there any guidelines or rules for the calculation of such fines or the imposition of sanctions?

Under Law 5160/2024, sanctions for violations of cybersecurity obligations include both administrative fines and corrective or supervisory measures, such as warnings, binding instructions, orders to remedy deficiencies and security audit requirements.

In terms of financial penalties, essential entities may be subject to fines of up to EUR 10 million or 2% of their total worldwide annual turnover, whichever is higher, while important entities may face fines of up to EUR 7 million or 1.4% of their total worldwide annual turnover. Additional supervisory measures may also be imposed depending on the nature and severity of the infringement.

With regard to data protection, the GDPR provides for administrative fines of up to EUR 20 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. In addition, Law 4624/2019 provides for supplementary provisions, including potential criminal sanctions and civil liability, depending on the circumstances of the infringement.

As regards the calculation and imposition of fines, both frameworks follow a case-by-case and proportionality-based approach. In particular, fines must be effective, proportionate and dissuasive. Under the GDPR, supervisory authorities take into account factors such as the nature, gravity and duration of the infringement, the degree of responsibility of the controller or processor, whether the infringement was intentional or negligent, the number of data subjects affected, actions taken to mitigate damage, the level of cooperation with the authority and any previous infringements. The methodology for calculating administrative fines is further guided by the European Data Protection Board, including Guidelines 04/2022, as well as relevant guidance and practice of the Hellenic Data Protection Authority.

47. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Enforcement decisions issued by competent authorities in Greece are subject to judicial review.

Under GDPR (Article 78) and Law 4624/2019, natural and legal persons have the right to an effective judicial remedy against legally binding decisions of supervisory authorities, including decisions of the Hellenic Data Protection Authority.

Under Greek administrative law, decisions imposing administrative sanctions (including those issued by the National Cybersecurity Authority pursuant to Law 5160/2024) may be challenged before the competent administrative courts. In practice, appeals against decisions of independent authorities are typically brought before the administrative courts of first instance or, in certain cases, directly before the Council of State, depending on the nature of the act.

Such remedies allow for a full review of the legality of the decision, including both procedural and substantive aspects.

Contributors

Dr. Themistoklis Giannakopoulos
Partner, Head of TMT & Data
themistoklis.giannakopoulos@gr.andersenlegal.com

Nicholas Zelios
Director
nikos.zelios@gr.andersenlegal.com

Olga Fakiola
Senior Associate
olga.fakiola@gr.andersenlegal.com