Legal 500
Country Comparative Guides 2025

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

Kleio Kondi

Associate | kleio.kondi@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'),

It is noted that, pursuant to Article 84 of Law 4624/2019, a significant number of provisions of Law 2472/1997 are repealed while its provisions referred to in that article are retained.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 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,
- Law No 5002/2022 on waiving the confidentiality of communications, cybersecurity and protection of citizens' personal data.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2025 - 2026 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments)?

On November 27, 2024, Greece enacted Law 5160/2024, aligning its national legislation with the EU's NIS2 Directive (Directive (EU) 2022/2555). Entities affected by Law 5160/2024 need to devise and present appropriate cybersecurity measures to ensure compliance. This

means that by late February 2025, affected organizations are expected to have their cybersecurity frameworks aligned with the new requirements.

3. 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?

Following the application of the GDPR certain obligations under the previous Law 2472/1997 were abolished. For instance, under the previous legal framework, there was an obligation to notify the Hellenic Data Protection Authority (hereinafter, 'HDPA') for establishing and operating a non-sensitive personal data file and for performing such processing. Moreover, article 7 of Law 2472/1997 provided for a licensing procedure on the processing of sensitive personal data.

In addition, according to the decision No 46/2018 of the HDPA *"the provisions of Article 7 of Law 2472/1997, insofar as they provide for an authorization of the (Hellenic) Data Protection Authority, are no longer applicable from 25.05.2018 onwards as contrary to the GDPR, which is directly applicable, given that the categories of data, referred to in this Article of the national law, do not coincide with those referred to in Article 9 (4) of the GDPR. Therefore, the Authority is no longer competent to issue authorizations for the processing and for the establishment and operation of a file based on Article 7 of Law 2472/1997"*.

However, for each entity appointing a Data Protection Officer in accordance with Article 37 of the GDPR there is the requirement of formally announcing the competent person/entity before the HDPA in accordance with the procedure established to this respect through its website.

From a cybersecurity standpoint, entities falling under article 4 of the relevant legislation are required to conduct a self-assessment to determine whether they qualify as essential and important entities under the provisions of Law 5160/2024. Following this, they must complete their self-registration in the NCSA registry, where specific service providers (outlined in article 19) must also register, at the below-mentioned deadlines and provide details on the entity's identity, sector of activity, and cybersecurity measures in place.

More specifically, the Ministry of Digital Governance has issued the Ministerial Decision no 1381/2025 (Government Gazette Issue no 463/10-02-2025) for the establishment of a digital platform to facilitate the above registration of such entities, as outlined in Articles 4 and 19 of the Law 5160/2024. The following deadlines for the submission of required information are specified:

- All entities classified as essential and important under Law 5160/2024 are required to submit the necessary information to the NCSA by the updated deadline of April 11, 2025, which was initially set for January 27, 2025.
- Specific Service Providers: Entities listed in Article 19 of Law 5160/2024 must submit the relevant information by the revised deadline of March 28, 2025, originally set for January 17, 2025. These entities include: Domain Name System (DNS) providers, Top-Level Domain (TLD) registries, Domain name registration service providers, Cloud service providers, Data center operators, Content delivery network providers, Managed service providers, Managed security service providers, Online marketplaces, search engines, and social media platforms.

Notwithstanding, pursuant to article 30 of L.5160/2024, specific entities engaged in activities related to national security, public order, defense, or law enforcement, including activities concerning the prevention, investigation, detection, and prosecution of criminal offenses, or those providing services exclusively to public administration entities referred to in paragraph 6 of Article 3, may be exempted from the obligations set forth in Article 4, subject to the conditions and requirements established by a joint ministerial decision.

Furthermore, law 5160/2024 does not establish a specific licensing process for covered entities. However, entities must comply with all cybersecurity standards and requirements the law sets. Entities that fail to comply with the cybersecurity obligations set forth in the relevant legislation, including the registration obligation described above, might face administrative fines or other corrective actions regulated in articles 24-26 of the aforementioned law.

4. How do the data protection laws in your jurisdiction define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data")? Do such laws include a specific definition for special category or sensitive personal data? What other key definitions are set forth in the data protection

laws in your jurisdiction (e.g., "controller", "processor", "data subject", etc.)?

According to article 4 of the GDPR, personal data means 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 an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Furthermore, according to article 9 par. 1 of the GDPR, special categories of personal data ('sensitive' personal data) refer to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

In article 84 of Law 4624/2019, regarding the definitions, there is a clear provision for reference to article 2 of Law 2472/1997.

5. 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 of 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.

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.

6. 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.

7. 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?

Article 9 par. 1 of the GDPR introduces a general prohibition on the processing of special categories of personal data. However, par. 2 of the above article provides for specific requirements that must be met in order for the processing to be legal. Explicit consent by the data subject, carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, protecting the vital interests of the data subject or of another natural person, processing which is necessary in the course of legitimate activities with appropriate safeguards by a foundation, association any other not-profit body, processing relating to personal data which are manifestly made public by the data subject, the establishment, exercise or defense of legal claims, substantial public interest, the provision of health or social care or treatment, public interest in the area of public health, when processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, are all legal bases which can justify processing of special categories of personal data. In addition, Law 4624/2019 (Article 22) contains specific provisions for the processing of special categories of data, but according to the opinion of the Hellenic Data Protection Authority these are either a repetition of the provisions of the GDPR or are outside the authorization framework of the national legislator as provided by the GDPR.

Furthermore, paragraph 3 of the abovementioned article 22 provides for an explicit obligation to take appropriate and specific measures in the processing of specific categories of personal data in order to safeguard the data subject's interests.

Moreover, article 9 par. 4 of the GDPR provides for the possibility of Member States to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Pursuant to the aforementioned possibility provided by the GDPR, article 23 of Law 4624/2019, introduces a general prohibition on the processing of genetic data for health and life insurance purposes.

Additionally, Law 4624/2019, elaborating on the provisions of Article 9 (2) of the GDPR 2016/679, provides in Article 22(1) that the processing of health data is permitted by public and private entities, provided that it is necessary:

- for the exercise of rights arising from the right to social security and social protection and to fulfill related obligations
- for preventive medicine, for assessing an employee's working capacity, for medical diagnosis, for the provision of health or social care, or under a contract with a health professional or other person subject to professional secrecy or under his supervision; or
- for reasons of public interest in the area of public health, such as serious cross-border threats to health or to ensure high standards of quality and safety of healthcare and medicines or medical devices, in addition to the measures referred to in the second subparagraph of paragraph 3, the provisions ensuring professional secrecy as provided by law or a code of ethics must be observed.

Paragraph 2 of Article 22 of Law 4624/2019 provides that the processing of health data is exceptionally permitted by public bodies, provided that it is necessary:

- strictly necessary for reasons of substantial public interest
- necessary to prevent a significant threat to national security or public safety or
- is necessary to take humanitarian measures, and in such cases the interest in processing outweighs the interest of the data subject.

In addition, during the lawful processing of health data by both public and private entities, all appropriate and specific measures must be taken to safeguard the interests of the data subject.

8. 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, exclusions or limitations described above there are also general limitations of the material scope of the GDPR. In particular, the GDPR does not apply to the processing of personal data:

a. in the course of an activity which falls outside the scope of Union law,
b. by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU,
c. by a natural person in the course of a purely personal or household activity,
d. By competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

What is more, the scope of the GDPR does not apply on anonymous data. More precisely, information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identified, is not subject to the GDPR provisions. The above exception does not cover cases of pseudonymous data, which is still subject to EU data protection laws. Law 4624/2019 basically repeats the aforementioned condition under (c) above.

9. Does your jurisdiction require or recommend 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.

10. Are there any specific codes of practice 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.

11. 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.

12. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? 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.

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

Article 36 of the GDPR refers to the controller's obligation to consult the supervisory authority. In particular, article 36 par. 1 provides that the controller shall consult the supervisory authority prior to processing where a data protection impact assessment (hereinafter, 'DPIA') indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

In addition to the above, obligatory consultation of the supervisory authority may arise under article 31 of the GDPR, as well as in the case of a personal data breach under article 33 par. 3 (b) of the GDPR.

14. 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, 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 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.

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.

15. 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).

Law No 4624/2019 does not stipulate explicitly employee training. However, the HDPA has highlighted the significance of employee training through its caselaw. More specifically, in its Decision 44/2019 employee training on data protection is identified -amongst others in a non-exhaustive list- as a measure of compliance with accountability principle, in accordance with Article 5 of the GDPR. Given also that all companies subject to audit by the HDPA shall demonstrate compliance with the principles established in Article 5, it results that employee training is an organizational measure towards this direction. Moreover, in the Decision 50/2021 the HDPA stated that with respect to a specific data processing the civil servants, as staff of the respective Ministry, had not received appropriate guidance or training, implying thus the relevant obligation of the data controller. In a recent Decision No 10/2024, the HDPA imposed one of the highest fines ever of almost 3.000.000 euros on a Data Controller for leak of personal data later published on the dark web due to a ransomware attack. Therein, it is worth noted that staff training aiming at better handling data breach incidents was an argument invoked by the Data Controller before the HDPA to demonstrate compliance measures that have been implemented following the incident. The HDPA upon its assessment when calculating the fine identified the technical and organizational measures that have been taken following the incident amongst the mitigating factors.

Additionally, considering the constant developments on this dynamic area of law, it is highly recommended for all

organizations subject to GDPR to engage into training of staff involved in processing operations, in a systematic manner (i.e., at least annually). This pattern forms a consistent approach and serves for the entities as a proactive organizational measure, demonstrating compliance with the GDPR requirements.

16. 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 the right to inform the data subjects is subject to more fairness and transparency as part of the accountability principle applying on data controllers. The HDPA has already conducted ex-officio investigations on the compliance of data controllers with the requirements of the GDPR and data protection in electronic communications. Within this context the HDPA audited the information provided to data subjects on the websites through relevant privacy notices sections, as per their content, in accordance with articles 13 and 14 of the GDPR. Therefore, it results that websites are also subject to compliance with the information obligation towards the data subjects.

The information to be provided towards the data subjects should include the identity and the contact details of the controller and, where applicable, the controller's representative; the contact details of the data protection officer, where applicable; the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; where the processing is based on the legitimate interests pursued by the controller or by a third party; the recipients or categories of recipients of the personal data, if any; where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the respective applicable safeguards to this respect; the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; when processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; the right to lodge a complaint with a supervisory authority; whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. In case, the information have not been obtained from the data subjects, additional information on the type of data concerned and the source of origin should be provided.

To this end, Law 4624/2019 includes additional derogations -to the ones already stipulated in the GDPR- from the information obligation towards the data subjects when data is collected from another source and not directly from the latter, i.e. for reasons of national or public security and the establishment, exercise or defense of legal claims of the data controller as the case may be. The HDPA's Opinion on Law 4624/2019 has already highlighted that these provisions are not specified as required by the GDPR. Therefore, it will be assessed on a case-by-case basis whether these provisions contravene the GDPR and the existing legal framework arising from the European Convention of Human Rights and the Charter of Fundamental Rights of the European Union.

17. Do the data protection laws in your jurisdiction draw any distinction between the responsibility of controllers and the processors of personal data? If so, what are the implications?

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.

18. 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.

19. Please describe any restrictions on targeted advertising and/or behavioral advertising. How are these terms or any similar terms defined?

Targeted advertising is a marketing practice also including behavioral advertising. These terms are not defined as such in the existing legislative texts.

However, the HDPA in its website, provides that targeted advertising usually takes place through cookies and online behavioral advertising. In Greek legal framework the provisions of law 3471/2006 as mentioned above apply with respect to cookies, requiring the consent of the user following the latter's clear and detailed information for the storage of data or gaining access to information already stored in the terminal equipment of the user.

By way of derogation, any technical storage or access required for the conveyance of information through an electronic communications network, or which is necessary for the provision of information society services explicitly requested by the user can be installed without the user's consent to this respect. The HDPA has also issued recommendations on best compliance practices for data controllers with the requirements on trackers and related technologies management. Targeted advertising based on trackers of such kind is subject to the same limitations as already provided in the law and further practically elaborated in the HDPA's recommendations. Trackers which are not necessary for the technical operation of the site, may under no circumstances be used without the prior explicit consent of the user and therefore, cannot be included in the “technically necessary" trackers requiring no consent. Future developments on E-Privacy sector will naturally be reflected on a national level as per the conditions and management of said technologies.

20. Please describe any data protection laws in your jurisdiction restricting the sale of personal data. How is the term “sale" or such related terms defined?

The HDPA has dealt with the issue of personal information sale under the previous legislative framework prior to the GDPR. More specifically, it has issued the

Decision 26/2004 wherein it recognized that the collection of personal data for the purposes of direct marketing and promotion of sales and products, whether or not concluded on a professional basis, is lawful under specific circumstances. The consent of the data subject is required to this respect or by way of derogation, the processing can be justified as lawful on the basis of the legitimate interests pursued by the Data Controller. However, for this derogation to be invoked, the following conditions should be fulfilled: the personal data are available through public sources for which the data subjects have provided their consent in order to be included, or the relevant lawful conditions for their inclusion in publicly available sources have been safeguarded, or the data subject has made public the latter's personal data for similar purposes. It is further specified that the personal data justified to be used for this purpose include the full name, post address and profession of the data subject. The HDPA in the past and prior to the GDPR had conducted audits on companies active on drafting and selling lists with personal data and subsequently imposed the relevant fines, while further proceeded for the impositions of relevant criminal sanctions by the competent authorities. The aforementioned Decision has been also invoked by the HDPA in a more recent Decision relating to the subject matter (i.e. Decision No 100/2014, confirming thus the conditions as set above for the processing to be considered legitimate.

Under the current legislative framework, it remains to be seen how this era will be formulated, provided that the conditions of lawfulness of processing are now stricter.

21. Please describe any data protection laws in your jurisdiction restricting telephone calls, text messaging, email communication, or direct marketing. How are these terms defined?

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') sets the rules and restrictions for unsolicited email, SMS and telephone communications.

One such restriction is: "The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail, for the purposes of direct marketing of goods or services, or any advertising purposes, may only be allowed in respect of subscribers who have given their prior consent."

Furthermore, unsolicited calls with human intervention for purposes of direct marketing are not allowed when the subscriber has previously declared that he/she wishes not to receive such calls either before the provider of the publicly available service or before the specific data controller concerned.

On the other hand and by way of a derogation, the e-mail and SMS contact details that have been lawfully obtained in the context of the sale of a product or a service or other transaction can be used for direct marketing of similar products or services by the supplier or the fulfilment of similar purposes, even when the recipient of the message has not given his/her prior consent, provided that he/she is clearly and distinctly given the opportunity to object, in an easy manner and free of charge, to such collection and use of electronic contact details upon collection and on the occasion of each message in case the user has not initially refused such use.

Law No 3471/2006 remains valid and applies as lex specialis in relation to the GDPR on these matters. It is also worth noted that with regards to the electronic consent in the context of Law No 3471/2006 the HDPA has adopted the Directive No 2/2011 in order to provide some guidance and good practices in relation to the aforementioned derogation for the purposes of direct marketing

22. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined?

Pursuant to article 4 par. 14 of the GDPR, biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

The biometric data belong to the special categories of personal data and their processing is regulated in Article 9 of the GDPR and Article 22 of Law 4624/2019.

Moreover, Article 9 par. 4 of the GDPR provides for the power of Member States to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Law 4624/2019 does not contain any specific provisions regarding the processing of biometric data.

In addition, prior to the implementation of the GDPR, the HDPA had issued a number of decisions regulating

specific issues of biometric data processing, the following decisions are illustrative:

- Decision No. 42/2024 – Ex officio investigation and complaints submission before the HDPA for a system of restricted access in facilities processing biometric data. The violations related to lawfulness principle and the obligation to conduct a Data Processing Impact Assessment with regards to the system.
- Decision No. 13/2024 – Ex officio investigation for the development and installment of certain programmes by the competent Ministry with regards to the audit of Facilities/ Temporary Receptions of third countries citizens, also including processing of their fingerprints as biometrics.
- Decision No. 57/2022 – Reprimand and order for compliance on a company for violations of accountability principle and transparency principle with regards to biometric data processing.
- Decision No. 17/2014 – Approval of pilot biometric system for research purposes.
- Decision No. 127 / 2012 – Prohibition on the installation and operation of a biometric system for monitoring the observance of working hours.
- Decision No. 81/2012 – Installation of a closed-circuit television and biometric input / output control system for workers in a drug warehouse.
- Decision No. 57/2010 – Approval of the operation of two pilot biometric systems exclusively for research purposes.
- Decision No. 31/2010 – Pilot biometric access control system at critical facilities of Thessaloniki International Airport 'Macedonia'.

More specifically, on the issue of data processing at work, the HDPA in Directive 115/2001 previously stated that the collection and processing of personal data of employees for purposes that do not directly or indirectly affect the employment relationship is prohibited. The consent of the employees cannot form the legal basis for circumventing the prohibition on exceeding the purpose. In Chapter E, paragraph 3 of the abovementioned Directive, more extensive reference is made to the processing of biometric data in the context of employment relationships. Additionally, due to their nature when data processing includes this kind of data, it is highly likely that a DPIA in accordance with the relevant national list of the HDPA will be required prior to the processing concerned.

23. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

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.

24. Is the transfer of personal data outside your jurisdiction restricted? 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?)

Transfers to third countries can take place if there is a Commission Adequacy Decision or other appropriate safeguards such as BCRs, standard contractual clauses duly adopted and approved, legally binding and enforceable instruments between authorities or bodies, approved code of conducts or certification mechanisms. In the absence of an adequacy decision or of appropriate safeguards, derogations can be used to frame the data transfers as below mentioned:

- consent of data subject,
- performance of a contract, with further nuances to this respect,
- the transfer is necessary for important reasons of public interest,
- the transfer is necessary for the establishment, exercise or defence of legal claims,
- transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent,

- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case. As an exception to the previously mentioned derogations compelling legitimate interests are also foreseen in cases when transfer is not repetitive and concerns a limited number of data subjects.

Under the GDPR, the HDPA has clarified that the issuance of a national license is not required when transfers are governed by Commission Adequacy Decisions or by appropriate safeguards as aforementioned, unless they are ad hoc contractual clauses between data importers and data exporters, or they concern administrative provisions between public authorities, also including enforceable and substantial rights of the data subjects, such as Memorandum of Understanding. In the last case, a license is required since the administrative arrangements of such kind are not legally binding.

Furthermore, for the BCRs, since they are now approved under the cooperation mechanism on a European level, in accordance with the GDPR provisions, a national license by each national authority concerned is not required. Furthermore, the HDPA has specified that the derogations stipulated in the GDPR as a tool to govern international transfers should be interpreted strictly, without requiring the issuance of a license to this respect. However, if the transfer is based on the compelling legitimate interests of the data controller provided that all conditions foreseen to this respect are fulfilled, the HDPA should be informed on the transfer and additional information should be further provided to the data subject to this respect. Furthermore, the HDPA has also specified that any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer.

In legal practice, the most common tool to address intragroup data transfers across the world is the BCRs. In the event where transfers take place in a more limited way, standard contractual clauses are also used.

On 27th of June 2021 the new sets of standard contractual clauses of the European Commission entered into force, echoing GDPR's requirements, along with the Court of Justice of European Union's remarks on Schrems II which invalidated Privacy Shield. With the use of a multi modular approach governing different types of transfers, i.e. from data controller to data controller, from data controller to data processor, from data processor to data processor and from data processor to data controller, the new sets of standard contractual clauses should replace within an eighteen month transitional period the previous ones, while since 27th of September 2021 it is no longer possible to rely upon the previous sets.

With respect to the transfer of data to the US, since July 2023, a new adequacy decision for safe and trusted EU-US data flows has been adopted, the so-called EU-US Data Privacy Framework. The safeguards that have been put in place by the US Government in the area of national security (including redress mechanism) apply to all data transfers under the GDPR to companies in the US, regardless of the transfer mechanisms used. Therefore, the use of other tools such as BCRs or SCCs is also facilitated.

Law 4624/2019 only comments on international transfers within the context of Directive's 2016/680 implementation regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. General principles governing such transfers, appropriate safeguards and derogations apply.

25. 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.

26. 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 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 the 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 an 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.

27. 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.

GDPR provisions calling for more fairness and transparency provide for the following rights:

- **Right to information**: right to precise information about data processing;
- **Right of access:** confirmation about processing of personal data and access to specific relevant information;
- **Right to rectification:** rectification of inaccurate data and complete incomplete data;
- **Right to erasure:** erasure of data which is no longer necessary under certain circumstances;
- **Right to restriction of processing:** when data accuracy is challenged, processing is unlawful, data is no longer necessary or when the data subject objects to processing;
- **Right to data portability:** the data subjects can request under certain conditions to either receive in a specific format the data belonging to them or to directly

transfer it to another data controller;
- **Right to object:** the data subject can object to processing when this relies upon the legitimate interests of the data controller or public interest;
- **Right to human intervention:** in cases where exclusively automated processing takes place, including profiling, the data subject may express one's point of view and contest the decision taken based on this processing.
- **Right to withdraw consent:** when processing is relied upon consent, the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

The rights can be exercised through any possible means the data controller or data processor provides to this respect (i.e hard-copy forms, emails, by phone communication). The means should be easily accessible and understandable in order not to discourage the data subjects to proceed accordingly. The deadline provided under the GDPR for replying to such requests is one month from the submission of the request, which can be further extended for two more months, where necessary, considering the complexity and number of the requests. All information and communications made to this purpose by data controllers shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request.

The right to be informed, right of access and right to object are also provided in HDPA's Directive for the use of CCTV (Directive 1/2011) with respect to the protection of persons and goods regarding personal data collected by CCTV systems. The time limit to satisfy the right of access in this case, in the HDPA's Directive prior to the GDPR was fifteen (15) days. The HDPA has further specified how the right to be informed can be satisfied through relevant signs, whereas it has also underlined that when for instance a copy of the footage is provided to data subjects exercising their right of access, third parties should be covered, i.e. by partially blurring the image, provided that their right to privacy is violated.

Moreover, rights arise from Law 3471/2006, such as the right of data subjects to be informed with respect to call recording, and the right of data subjects to be informed about processing of location and traffic data on the basis of consent. Furthermore, the data subjects have the right to object the inclusion of their personal details on a hard copy or electronic public registry and rights related to call identification and potential restrictions thereof. Moreover, the data subjects reserve the right not to receive detailed accounts and to impede the automatically forwarded calls from third parties to their device, while specific provisions apply with respect to cookies.

Law 4624/2019 introduces certain restrictions on the satisfaction of rights of access, correction, erasure and the right to object as provided by the GDPR under certain conditions. Additionally, a derogation from the obligation of communication towards the data subjects in the case of a data breach is foreseen where information due to their nature or the compelling legitimate interests of a third party should remain confidential. As already mentioned, the HDPA has commented that these additional restrictions are not duly specified as required by the GDPR. Therefore, it will assess within the context of exercising its powers whether such restrictions comply with the GDPR and the existing legal framework arising from the European Convention of Human Rights and the Charter of Fundamental Rights of the European Union.

28. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

Article 40 and 41 of Law 4624/2019 provide for judicial protection against a data controller or processor, stipulating the competent courts before which a relevant lawsuit should be filed. The law also provides for the possibility of exercising the right to lodge a complaint with a supervisory authority and the right to an effective judicial remedy against a supervisory authority through a non-profitable association, organization etc. It should be further noted that under Law 4624/2019 the Decisions and individual administrative Acts of the HDPA, including the Decisions imposing sanctions, are challenged before the Council of State. This provision has been widely challenged by practitioners, considering the costs and the great amount of time this level of justice requires in Greece.

Furthermore, according to Law 3471/2006, data subjects whose rights are violated may ask for compensation for any financial damage caused to them. Even injury of feelings triggers claims for compensation.

29. 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 Law 3471/2006 transposing E-privacy Directive if injury of feelings takes place, an obligation for compensation for injury of feelings also arises. According to article 14 of Law 3471/2006, compensation for injury of feelings is awarded irrespectively of any potential financial damage requested.

This establishes the presumption of civil liability of the data controller when a violation of the legal framework takes place, further leading to compensation of data subjects for injury of feelings. There is extended caselaw of the competent civil courts which have identified that the obligation for compensation for injury of feelings is sufficiently triggered by the violation of the legal provisions concerning data protection on electronic communications, since such action directly undermines the right of privacy and the protection of data subject's personality.

It should be also mentioned that the HDPA in its relevant Opinion on Law 4624/2019 has commented that the sanctions provided by Law 3471/2006 -which further refer to the sanctions system of Law 2472/1997- should be harmonized with the ones provided by the GDPR for the sake of consistency and efficiency.

In any case, Article 82 of the GDPR is directly applicable, providing that any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

30. How are data protection laws in your jurisdiction typically enforced?

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.

31. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

With regard to the extent of the administrative fines threatened, the delimitation of which depends on the nature and specific circumstances of each infringement, the GDPR provides the amount of up to EUR 20,000,000 or, in the case of enterprises, the amount of up to 4% of the total world annual turnover of the preceding financial year, whichever is higher. The orders of the regulators are subject to appeal before the competent administrative Courts.

Furthermore, with regards to the criminal sanctions provided for in article 38 of Law 4624/2019, these vary in terms of severity depending on the specific circumstances of each offense. Article 40 of the same law provides for civil liability as explained above.

32. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

Law 4624/2019 provides for some thresholds on fines depending on the violation of the framework. More specifically, in article 39 of the Law a maximum 10.000.000 million Euros fine on data controllers of public sector is provided for certain violations. However, upon conclusion of the respective decision and the fine's determination, certain factors should be taken into account in each individual case, echoing thus article 83 of the GDPR (i.e. the intentional or negligent character of the infringement, any relevant previous infringements by the controller or processor etc).

The HDPA has not issued any specific guidelines regarding the calculation of fines or thresholds for the imposition of sanctions. However, through its recent caselaw the HDPA has assessed in practice all factors that are mentioned in article 83 of the GDPR. These details are now further framed and interpreted in the Guidelines No. 04/2022 of the European Data Protection Board on the calculation of administrative fines under the GDPR which were adopted in May 2023. This serves as a point of reference when calculating relevant fines, since they were also invoked in recent Decision No 10/2024 of the HDPA.

Additionally, in Law No 3471/2006 on the protection of personal data and privacy in electronic communications which continues applying as lex specialis in relation with GDPR on certain matters, fines of up to 150.000 Euros are foreseen along with criminal sanctions. In cases where a risk on free operation of democratic regime or national security arises, along with the criminal sanctions a fine

from 50.000 to 350.000 Euros is foreseen.

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

Article 78 of the GDPR and article 20 of Law 4624/2019 explicitly provide for the possibility of a natural or legal person to lodge a judicial remedy against a legally binding decision of a supervising authority concerning them.

34. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

With regards to Data Privacy, in 2019 the HDPA within the context of its competences had proceeded with remote ex-officio investigations in order to assess the level of compliance and awareness of data controllers. In this action the competent DPA has focused on data controllers providing online credit/financial services, insurance services, e-commerce, ticket services and public sector services. These audits were mostly channeled towards certain regulatory requirements relating to transparency principle, use of cookies, mechanisms for newsletters and security of websites. Following this action, the HDPA proceeded with relevant recommendations and interventions where required. In 2022 this approach was once again selected by the HDPA when it audited websites of informative nature, on the basis of their visitors, with regards to the cookies banners and the options therein provided in relation to the use of cookies.

Furthermore, within its awareness competences, in 2023 the Hellenic DPA participated in a new project aiming at enhancing awareness on data protection over critical social and professional groups (kids and professionals on data protection). One of the main objectives of this project was the creation of a cooperation and exchange of views platform whereas Data Protection Officers and other professionals with relevant background exchange their views and expertise across various sectors, in order for the principles of data protection to be practically implemented. This project has proceeded to its full production phase with relevant awareness sessions across all stakeholders concerned. The HDPA has also participated in the completed coordinated enforcement of the supervisory authorities on the role of Data Protection Officers which started in early 2023. Amidst this action relevant audits in the public sector and more specifically, in Ministries, big Municipalities and specific public bodies were announced. It is also worth mentioning that the HDPA had previously (in 2022) participated in a similar coordinated enforcement action regarding the use of cloud services in public sector.

The current coordinated enforcement action for 2024 initiated by the European Data Protection Board is focused on the implementation of access right. This subject was selected following numerous complaints submitted before the competent authorities to this regard. The approach that will be followed by the authorities to this respect includes questionnaires for the organizations/ data controllers, official investigations and/or monitoring of the pending audits.

Moreover, ahead of the European Elections in June 2024, the HDPA has announced the initiation of investigation proceedings, following several complaints of Greek citizens living abroad for the receipt of relevant unsolicited email communications by candidates politicians. The investigation was followed by the relevant Decision No 16/204 that imposed fines upon the data controllers concerned (candidates and the competent Ministry to conduct the elections).

Very recently, the HDPA announced that it participates in the coordinated action of the European Data Protection Board with regards to the implementation of erasure right (article 17 of the GDPR). This action aims at enhancing effectiveness and cooperation between the Data Protection Authorities. This subject matter was chosen, provided that it is one of the most commonly exercised GDPR rights, following which the authorities receive complaints by data subjects. Thirty-two (32) authorities will participate in this initiative and following the contact with the DPOs may and the input received, may further decide the implementation of additional monitoring actions where required. The focus of the HDPA will be on data controllers processing personal data in the context of marketing strategies consisting of loyalty programmes or/and granting loyalty cards, encouraging thus the purchase of products and services through the provision of various privileges in exchange.

35. 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 details.

Yes, organizations in Greece are required to adopt appropriate technical, operational, and organizational

measures to manage cybersecurity risks under the Greek Law 5160/2024. More specifically, as stated in Article 15, para 2 of the same law, the necessary cybersecurity risk management measures encompass the following:

- risk analysis and information security policies and procedures,
- cybersecurity incident handling,
- business continuity planning,
- basic cyber hygiene practices and trainings for both management and employees.
- policies on the use of cryptography or encryption, and
- the implementation of multi-factor or continuous authentication solutions, or other appropriate security methods.

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

Under the Greek cybersecurity framework, entities operating in sectors covered by NIS 2 Directive must appropriately manage supply chain and supplier-related risks. This requires ensuring that cybersecurity measures extend to direct suppliers or service providers, whose services or products impact the entity's critical functions, therefore addressing risks arising from third-party relationships.

37. Do the cybersecurity laws in your jurisdiction impose information sharing requirements on organisations?

Entities falling within the scope of NIS 2 Directive and the relevant Greek law are able to exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks, where such information sharing:

a. aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;
b. enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities.

The exchange of information takes place within the framework of communities of essential and important entities and, where applicable, their suppliers or service providers. This exchange is carried out with due consideration for the potentially sensitive nature of the exchanged information. The essential and important entities shall promptly notify the National Cybersecurity Authority of their participation in the above information exchange framework, as well as their withdrawal from participation as soon as it occurs.

Information that is confidential under Union or national rules, such as business secrecy regulations, may be exchanged with the Commission and other competent authorities in accordance with this law, only to the extent that such exchange is necessary for the implementation of its provisions. The exchanged information shall be limited to what is relevant and proportionate to the purpose of the exchange. The exchange of information shall preserve the confidentiality of such information and protect the security interests and commercial interests of the entities involved.

38. 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, what are their legal responsibilities?

In accordance with Article 15 para 5 of L. 5160/2024, entities must appoint an Information and Communication Systems Security Officer (I.A.S.P.E.) who will serve as the primary point of contact with the National Cybersecurity Authority and will oversee the implementation and compliance with cybersecurity obligations. His duties include:

a. The management of all types of communications and interactions with the National Cybersecurity Authority,
b. The responsibility for internal coordination and ensuring the entity's compliance with the requirements of this article, as well as incident reporting requirements in accordance with Article 16 of the same law.

The necessary resources for performing such duties are provided by the relevant entity. The Information and Communication Systems Security Officer must possess an appropriate level of autonomy in decision-making, the authority to implement decisions across the entity's

organizational units, the responsibility to inform management bodies, and to coordinate the management of security incidents, as well as the implementation of business continuity and disaster recovery plans. However, his duties are incompatible with those of the Data Protection Officer (DPO) under Article 37 of Regulation (EU) 2016/679.

39. Are there specific cybersecurity laws / regulations for different industries (e.g., finance, healthcare, government)? If so, please provide an overview.

In the financial/banking sector, EU 2022/2554 Regulation on Digital Operational Resilience for the financial sector (DORA) is considered to be a sector specific Union legal act which also regulates cybersecurity matters regarding financial institutions. This Regulation constitutes lex specialis with regard to Directive (EU) 2022/2555 (NIS 2), as the provisions relating to information and communication technology (ICT) risk management, management of resilience testing, information-sharing agreements and ICT third-party risk should apply instead. Furthermore, Bank of Greece has issued relevant guidelines on cybersecurity management.

In communications, Law 5002/2022, for the lifting of communications secrecy, cybersecurity and data protection, and its recent amendments (Law 5046/29.07.2023), which among other matters also introduced provisions related to cybersecurity with the aim to enhance the country's level of cybersecurity. This law also provided a framework for the collaboration between the National Cyber Security Authority and the National Intelligence Service in order to monitor the threats-vulnerabilities of IT and communication systems.

Moreover, the Cyber Resilience Act (Regulation 2024/2847), published on 23 October 2024, sets uniform cybersecurity requirements for the entire lifecycle of products with digital elements, from design to distribution. This regulation places compliance obligations on manufacturers, importers, distributors and all persons involved in the manufacture or distribution of products with digital elements within the EU market and is complementary to the existing cybersecurity legislations, such as the NIS2 Directive.

40. What impact do international cybersecurity standards have on local laws and regulations?

Entities must take into account the most current and relevant international cybersecurity standards when implementing appropriate and proportionate technical, operational, and organizational measures to manage risks related to the security of network and information systems. Furthermore, under Article 17 of L. 5160/2024, the use of European and internationally accepted standards and technical specifications related to the security of network and information systems may be established by a decision of the Head of the National Cybersecurity Authority, after considering any relevant directions issued by the European Union Agency for Cybersecurity (ENISA) and without imposing or favoring the use of any specific type of technology.

41. Do the cybersecurity laws in your jurisdiction impose obligations in the context of cybersecurity incidents? If so, how do such laws define a cybersecurity incident and under what circumstances must a cybersecurity incident be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

According to law 5160/2024, essential and important entities are required to report any incident that has a significant impact on the provision of their services to the Computer Security Incident Response Team (CSIRT) of the National Cybersecurity Authority without undue delay, providing relevant information to help assess cross-border implications of the incident. Furthermore, as appropriate, the relevant entities must promptly notify their service recipients of significant incidents that could negatively affect the provision of those services ensuring that affected parties are aware of the cybersecurity threat and any corrective actions they may need to take. These entities shall provide, among other things, any information that enables the National Cybersecurity Authority to identify the cross-border impacts of the incident.

42. How are cybersecurity laws in your jurisdiction typically enforced?

Greek law 5160/2024 outlines enforcement measures for non-compliance imposed to essential and important entities for violations like not meeting cybersecurity requirements or failing to report incidents. These measures must be effective, proportional, and deterrent, taking into account the circumstances of each individual case. Sanctions against natural or legal persons for violation of the relevant provisions are imposed by a specially justified decision of the Head of the National Cybersecurity Authority, which is issued after a hearing following their summons.

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

The National Cybersecurity Authority, pursuant to Law 5086/2024 on its establishment (Article 4.i), exercises regulatory responsibilities and conducts inspections within the framework of compliance monitoring.

More analytically, under Article 23 of the L.5160/2024, in order to fulfill the duties of the National Cybersecurity Authority as outlined in this document, its designated employees have auditing powers and are specifically authorized to:

a. Visit, with or without prior notice, the entities
b. Inspect and collect information and data from mobile terminals,
c. Conduct investigations in the premises of the entities,
d. Carry out seizures, take or obtain documents,
e. Seal any professional premises, electronic or non-electronic documents during the inspection period.

In particular, for essential entities, the National Cybersecurity Authority has the power to conduct the following, in accordance with Article 25 of the above law:

a. On-site inspections and corrective oversight within and outside the premises,
b. Targeted Security Audits
c. Security scans
d. Requests for the necessary information to assess the risk management measures,
e. Requests for access to data,
f. Requests for evidence concerning the implementation of cybersecurity policies.

The above targeted security audits are based on risk assessments conducted by the National Cybersecurity Authority or the audited entity, or on other relevant available risk-related information.

The results of each targeted security check are made available to the relevant Directorate of the National Cybersecurity Authority.

44. What is the range of sanctions (including fines and penalties) for violations of cybersecurity laws in your jurisdiction?

In Accordance with the relevant articles 26 of L. 5160/2024 and 34, 36 of the NIS 2 Directive, sanctions for violation of the relevant cybersecurity provisions include non-monetary remedies (such as warnings, recommendations, and security audit orders) and administrative fines. Notably, if essential entities fail to implement risk management measures or report significant incidents, they may face fines of up to €10 million or 2% of their total worldwide annual turnover. Important entities can be fined up to €7 million or 1.4% of their total worldwide annual turnover, while lower penalties apply for other violations of the law.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

Yes, under Article 26 of law 5160/2024 the general terms for imposing administrative fines on essential and important entities, as well as the sanctions are outlined in detail, and in accordance with Articles 34 and 36 of Directive (EU) 2022/2555.

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

According to Article 26 para 3 of the above law, enforcement decisions imposing fines and any other sanctions may be challenged by filing an annulment request with the competent Administrative Court of Appeal.

47. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

The National Cybersecurity Authority of Greece has issued the National Cybersecurity Strategy 2020-2025, which includes the strategic goals of: (a) the development of a functional cybersecurity governance system, (b) critical infrastructures and securing new technologies, (c) incident management optimisation, fight against cybercrime and privacy protection, (d) a modern environment for cybersecurity investments with emphasis on the promotion of research and development, (e) capacity building, promoting information and awareness raising, and (f) evaluation and feedback.

Furthermore, cybersecurity educational projects have been recently launched, such as the “AKADIMOS” project, a key initiative by the Ministry of Digital Governance and the National Cybersecurity Authority (NCSA). This project is a significant part of Greece's cybersecurity strategy, aimed at addressing the growing skills gap in cybersecurity.

Contributors

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

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

Kleio Kondi
Associate
kleio.kondi@gr.andersenlegal.com