COUNTRY COMPARATIVE GUIDES 2024

The Legal 500 Country Comparative Guides

Greece

DATA PROTECTION & CYBERSECURITY

Contributor

Andersen Legal – Pistiolis – Triantafyllos & Associates Law Firm

Dr. Themistoklis Giannakopoulos

Partner, Head of TMT, Antitrust, Competition and Regulatory Practice | themistoklis.giannakopoulos@gr.andersenlegal.com

Nicholas Zelios

Senior Associate | 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 by them; 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It is noted that, pursuant to Article 84 of Law 4624/2019, a significant number of provisions of Law 2472/1997 are repealed while its provisions referred to in that article are retained.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 No 4577/2018, which implemented Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,
- Ministerial Decree No 1027/2019 which clarified issues related to the application and the process of Law 4577/2018,
- 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 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments (together, "data protection laws"))?

On a national level, we expect the implementation of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

3. Are there any registration or licensing requirements for entities covered by these data protection laws, and if so what are the requirements? Are there any exemptions?

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".*

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

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 are the principles related to the general processing of personal data in your jurisdiction? For example, must a covered entity establish a legal basis for processing personal data, or must personal data only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

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 general processing of personal data?

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.

7. 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)?

Consent can be provided in a hard copy or electronic version.

With regards to the content of the consent and the minimum requirements that must be met in order for it to be ''informed'', Working Party 29 (hereinafter, 'WP 29') supports that it is necessary to inform the data subject about certain elements that are crucial to make a choice. Therefore, the minimum information required for obtaining a valid consent is the following:

i. the controller's identity,
ii. the purpose of each of the processing operations for which consent is sought,
iii. what (type of) data will be collected and used,
iv. the existence of the right to withdraw consent,
v. information about the use of the data for automated decision-making in accordance with article 22 (2)(c)34 where relevant, and
vi. on the possible risks of data transfers due to

absence of an adequacy decision and of appropriate safeguards as described in article 46.

Regarding other information about the processing of personal data, reference can be made to the data controller's Privacy Notice.

Finally, the data controller shall record, in a secure manner, the information necessary to demonstrate the consent of the data subject.

In Directive 2/2011 of the HDPA certain provisions further explain and clarify how consent provided by electronic means within this context fulfills the conditions of validity. Amongst others and with regards to consent for receipt of emails through internet certain examples are provided as guidance. Data controllers should confirm that the user has access to this email address, either through an initial informative email to the email submitted as contact email, which contains certain information such as the purpose, the origin and all relevant information etc. Another option is the double opt-in which is recommended in cases where the consent provided also includes receipt of further services by the user, such as subscription to a webpage with password and username. In this scenario, certain details such as identity and origin of the sender should be included, in the initial confirmation email, along with the activation of consent for instance through an email to a specific address of the data controller, or through a respective URL. Validity of consent depends on activation of consent by the user. Withdrawal of consent should be possible. In this case, new confirmation of the user's access to the email is not required. Such consent should be recorded in a safely manner for purposes of evidence. Withdrawal of consent should be always available either via email or hyperlink.

8. What special requirements, if any, are required for processing sensitive personal data? Are any categories of personal data prohibited from collection or disclosure?

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.

9. How do the data protection laws in your jurisdiction address health data?

According to Article 9(1) of the GDPR, health data falls under the special category of personal data, the processing of which is prohibited in principle. By way of exception, the processing of this information is permitted in specific cases specified in Article 9(2).

Correspondingly, Law 4624/2019, elaborating on the provisions of Article 9(2)(b), (f), (g), and (h) 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.

10. Do the data protection laws in your jurisdiction include any derogations, 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.

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please describe how.

Children are recognized as a vulnerable group of data subjects, requiring thus enhanced protection.

With regards to the conditions applying on child's consent in relation to information society services, the threshold of sixteen (16) years old was introduced by the GDPR. More specifically, consent of a child above sixteen (16) was deemed valid, whereas below sixteen (16) years old, such processing shall be lawful only if and to the extent that consent was given or authorized by the holder of parental responsibility over the child. According to the GDPR, Member States may provide by law for a lower age for those purposes provided that such lower age is not below thirteen (13) years. Following the issuance of Law 4624/2019 the age limit of a child's valid digital consent in Greece is now lowered to fifteen (15) years old.

Moreover, the HDPA in line with the interpretation provided so far by WP 29 as also approved by the European Data Protection Board, further underlines that in cases of a child's consent, the language addressed to data subjects should be simple, explicit and understandable. Furthermore, under the light of the GDPR's Preamble and the Guidelines, automated decision-making, including profiling having legal effects on children or significantly affecting them is prohibited, although certain exceptions are allowed to this respect when appropriate safeguards have been put in place. Additionally, children's vulnerability should not be taken into advantage and children should always benefit from the absolute right to object to profiling for purposes of commercial promotion.

12. Do the data protection laws in your jurisdiction address online safety? Are there any additional legislative regimes

that address online safety not captured above? If so, please describe.

By virtue of Presidential Decree, No 178/2014 on the organization of Hellenic Police Services, the Division of Cyber Crime was established. Its mission includes the prevention, investigation and suppression of crime and antisocial behavior committed through the internet or other electronic media. This Division further consists of various departments covering the whole range of user's online protection and cyber security. One of them is the Unit of Minors Internet Protection and Digital Investigation which has the following responsibilities:

a. the detection and prosecution of crimes committed against children using the Internet and other means of electronic or digital communication and storage;
b. the investigation of online or electronic harassment cases (cyber bulling);
c. assisting the competent public services investigating cases under (a) and (b) above for which investigation on an expert basis is required.

It is also worth noted that very recently and under Law 5029/2023 on arrangements for the prevention and combatting violence and bullying at schools Article 6, a digital platform designed for this purpose was introduced. More specifically, students and their parents, or anyone bearing parental responsibility will have access to the platform in order to be able to submit anonymous or named complaints. This procedure is optional and further facilitates the submission of complaints without prejudice to other complaint procedures before the competent authorities.

This initiative aims at combatting school violence and bullying and within one week of operation, numerous complaints have been lodged. Competent persons to deal with the complaints are scientists (such as psychologists and social workers) composing four member committees which will undertake a supervisory role on dealing with incidents of such nature within the specific school unit, along with awareness initiatives.

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

The HDPA as an independent administrative authority as provided for in article 9A of the Hellenic Constitution and remains the main enforcer of the data protection laws as currently in force and mentioned above under question (1). The HDPA is also in charge of awareness towards everyone, including minors regarding their privacy in general and online and has a specific section on its website to this respect, dedicated to minors. Therein, it provides guidance on personal data, postings, online contacts and social media use in order to frame their operation and highlight the privacy settings that can be activated.

The Division of Cyber Crime as mentioned above with its specific Unit on Minors Internet Protection and Digital Investigation has specific competences, as arising by the Presidential Decree establishing its operation. The HDPA encourages the data subjects in general, not only minors, to further report incidents before the Police in order for the latter to proceed accordingly, as they trigger penal proceedings, whereas the HDPA power amongst others is to exercise its administrative authority through fines imposition, following complaints by data subjects or ex officio investigations.

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024–2025?

At this timing, we are (still) expecting the E-privacy Regulation which will replace the E-privacy Directive as mentioned above. Its purposes include enhancing security and confidentiality of communications (including content and metadata, eg. Sender, time, location of a communication) and defining clearer rules on tracking technologies such as cookies, as well as on spam. Its scope is intended to cover all market players using the internet, such as instant messaging apps and web-based e-mail services. Therefore, it results that the new set of rules will for sure have an impact on existing national legislation transposing E-privacy Directive, also extending across the online safety landscape currently in force.

Moreover, legislative developments are also expected with regards to the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. The EDPB has acknowledged the importance of the fight against child and has suggested improvements in order to resolve some issues in the original text.

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

Regarding the protection of personal data by design and by default, the HDPA refers to article 25 of the GDPR in conjunction with Recital 78 of the GDPR's Preamble.

According to the data protection by design principle, both while determining the means of processing and at the time of the processing itself, the data controller shall introduce and implement appropriate measures and use technology designed to implement data-protection principles. Such measures are pseudonymization of personal data which should take place as soon as possible (namely replacement of personal data with artificially identifying data), encryption (encryption of personal data so that only the authorized persons can read it), minimization of data processing and introduction of necessary safeguards, in a manner that the requirements set by the GDPR are met and the protection of the rights of the data subjects is ensured.

Moreover, according to the data protection by default principle, the data controller shall implement appropriate technical and organizational measures for ensuring that, by default, privacy is ensured and only personal data which necessary for each specific purpose of the processing are processed. This obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. Such measures shall ensure that by default, personal data are not made accessible without the individual' s intervention to an indefinite number of natural persons.

In addition, the HDPA mentions two examples of measures designed to implement the data protection by design and by default principles. In particular:

a. A social networking platform should be encouraged to define user profile settings in order to protect privacy as much as possible. Such protection is ensured when the user profile is by default not accessible by indefinite number of people and
b. The need for transparency with regards to the functions and processing of personal data in order for the data subject to monitor data processing and for the controller to create and improve security features.

16. Are controllers and/or processors of personal data required to maintain any internal 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.

17. 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.

18. Under what circumstances is a controller operating in your jurisdiction 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.

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under what circumstances? How are these risk assessments typically carried out?

Article 35 par. 1 of the GDPR provides for a controller' s obligation to conduct prior to processing a DPIA where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.

Article 35 par. 3 of the GDPR indicates certain types of processing which shall be regarded as ''resulting in high risk''.

The HDPA, in the exercise of its competences and pursuant to the relevant provisions, issued its Decision No 65/2018 by which it drew up and published a list of the types of processing which are subject to the requirement for a DPIA. It is noted, however, that the above list is not exhaustive and therefore, in case the requirements of article 35 par. 1 of the GDPR are met, the controller must conduct a DPIA and comply with all obligations arising from the GDPR. This list further supplements and specifies the respective Guidelines issued on DPIAs.

With regards to the method of conducting a DPIA, the GDPR provides certain flexibility in defining its exact structure and form, as it is not specified by detailed provisions. Nevertheless, article 35 par. 7 of the GDPR provides that the assessment shall contain at least a systematic description of the envisaged processing operations and the purposes of the processing, an assessment of necessity and proportionality of the processing operations, an assessment of the risks to the rights and freedoms of data subjects, as well as the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR.

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, and 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, the Ministerial Decree 1027/2019 provided for the appointment of an Information and Network Security Officer by any organization falling under the scope of application of Law No 4577/2018, which implemented Directive (EU) 2016/1148. Each organization must immediately notify the National Cybersecurity Authority of the contact details of the Officer, following their appointment.

His responsibilities include communicating and collaborating with the National Cyber Security Authority and the relevant CSIRT, supervising the organization in terms of the obligations arising from the legislation in force, monitoring the implementation of the Uniform Security Policy, coordinating the training and awareness of employees, and drafting the organization's self-assessment report. Their role is proposed to be independent and not in conflict with other roles they may have inside the organization.

Although not expressly provided for, the role of the Information and Security Officer is advisory, and they do not have personal liability for non-compliance with the requirements of the relevant legal framework.

Additionally, Law 4961/2022 provides for the appointment of an IT and Communications Systems Security Officer and one deputy in each central government entity. This role is to be undertaken by an existing IT employee and the appointment is finalized by the decision of the competent Minister or a competent administrative body. Their duties are incompatible with those of the DPO and they may exercise other duties, as long as there is no conflict of interest. As it stands, the IT and Communications Systems Security Officer and the deputy are not personally liable, although the possibility of disciplinary sanctions cannot be ruled out as they report directly to the highest level of management of the respective entity.

Their responsibilities include demonstrating care for the security of network and information systems, cooperating with the competent cybersecurity bodies, being alert for the application of guidelines, requirements and measures, keeping a record with any IT and communications infrastructures and any software in use, participating in audits to verify the existing level of security, monitoring compliance with the organization's IT and communications systems security policy, and carrying out evaluations of the organization's cyber security level in cooperation with the competent authorities.

21. 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).

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 the very recent Decision 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.

22. 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.

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

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.

24. Do the data protection laws in your jurisdiction place obligations on processors by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal data?

In Greece, provisions on the respective requirements in cases of processing carried out on behalf of the data controller are specified under the GDPR. The data processors should guarantee the implementation of appropriate technical and organizational measures along with the confidentiality obligation of the persons authorized to process the data, the assistance in the exercise of rights from the data subjects, provisions on deletion or return of personal data following termination of service provision, making available to the controller all information necessary to demonstrate compliance, prior general or specific authorization for further engagement of data sub processors and performance only upon relevant orders and instruction of the data controller. Furthermore, assistance of the controller is also foreseen with respect to the obligations relating to data breach incidents and DPIAs. The respective assignment is concluded in writing and should precise the scope, duration, nature, purpose of processing, type of data, categories of data subjects, relevant obligations and rights of the contracting parties.

Law 4624/2019 does not include any further provisions to this respect.

25. Are there any other restrictions relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

Law 4624/2019 does not impose additional restrictions with respect to the appointment of processors. However, under the light of the requirements provided for in Article 28 of the GDPR, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

To this end, it is highly recommended for the controllers to proceed with an initial due diligence, privacy and security assessment of the partner, as a precondition of approval of the partnership, especially in cases where personal data processing of high risk for any reason (nature, scale etc) is involved. During the mandate of the assignment of data processing, the data controller has in any case an obligation to proceed with audits on the processor in order to ensure compliance with the requirements set out by the framework. The above audits are also aligned with the accountability principle which forms a fundamental concept in the GDPR.

26. 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 terms defined, and what restrictions on their use are imposed, if any?

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.

27. Please describe any restrictions on targeted advertising and/or cross-contextual behavioral advertising. How are these terms or any similar terms defined?

Targeted advertising is a marketing practice that includes contextual advertising and behavioral advertising. Contextual advertising is based on the content of the webpage the users are visiting or the keyword they have entered in a search engine, while behavioral advertising is based on observing their behavior. These definitions derive from a study conducted by DG for Internal Policies of the EU Commission, dated September 2021, entitled “Regulating targeted and behavioral advertising in digital services. How to ensure users’ informed consent”.

Targeted advertising usually takes place through cookies. 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 Regulation will naturally be reflected on national level as per the conditions and management of said technologies.

28. Please describe any data protection laws in your jurisdiction addressing the sale of personal data. How is the term “sale” or such related terms defined, and what restrictions are imposed, if any?

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. 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.

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.

29. Please describe any data protection laws in your jurisdiction addressing telephone calls, text messaging, email communication, or direct marketing. How are these terms defined, and what

restrictions are imposed, if any?

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 with 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.

30. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined, and what restrictions are imposed, if any?

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. 13/2024 – Ex officio investigation for the development and installment of certain programs 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.

31. 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.

32. 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 interested party 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 the 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 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.

33. What security obligations are imposed on data controllers and processors, if any, 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.

34. Do the data protection laws in your

jurisdiction address security breaches and, if so, how do such laws define a "security breach"?

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.

Additionally, the main national framework on cybersecurity is Law 4577/2018 which transposed Directive 2016/1148 refers on "incidents" meaning any event having an actual adverse effect on the security of network and information systems, reminding that whereas all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches.

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

The issue of information security is regulated by several provisions both on European and national level.

Specifically, Article 32 of the GDPR makes explicit reference to the security of data processing, and in particular the implementation of appropriate technical and organizational measures by both controllers and processors.

In addition, Article 28 of the GDPR contains specific provisions (par. 3 (c) and (f)) that regulate processing security issues by the processor, while emphasizing the responsibility of the controller (par. 1) for cooperation only with processors which can ensure a strong level of security, in line with the requirements set by the GDPR.

It is noted that on a national level in Article 12 of Law 3471/2006 on the protection of personal data and privacy in the field of electronic communications, it is envisaged that the provider of electronic communications services must take appropriate technical and organizational measures in order to protect the security of the services provided, as well as security of the public electronic communications network.

It is further noted that at European level, Directive 2016/1148 (NIS) contains provisions on measures to achieve a high level of security of network and information systems jointly throughout the European Union. The Directive has been transposed into Greek legal order by Law 4577/2018.

Other specific provisions regarding security requirements are included in sector specific legislation, i.e. in the telecoms sector (i.e. Law 3674/2008, ADAE Regulation for the Assurance of Confidentiality in Electronic Communications, ADAE Regulation governing security and integrity of electronic communication networks and services). The Hellenic Authority for Communication Security and Privacy (ADAE) has been established according to article 19 par. 2 of the Hellenic Constitution. According to article 1 of its founding law, 3115/2003, its purpose is to protect the free correspondence or communication, as well as the security of networks and information in any possible way. Other specific provisions regarding security requirements are included in Law 4961/2022 regarding the use of AI technologies, such as the obligation of conducting an Algorithmic Impact Assessment.

The HDPA and ADAE take the issue of information security seriously and have in fact imposed administrative fines for inadequate security measures.

36. Under what circumstances must a business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable regulator in your jurisdiction, and what is customary in this regard in your

jurisdiction?

When a security breach includes personal data breach the following provisions apply. The HDPA, when it comes to a personal data breach, refers to the provisions of the GDPR and in particular, to articles 33 and 34 of the GDPR regarding the obligation of the controller to notify the breach to the supervisory authority and to communicate the breach to the data subject.

According to article 33 of the GDPR, data controllers, in the case of a personal data breach which is likely to result in a risk to the rights and freedoms of natural persons shall without delay and within 72 hours after having become aware notify the breach to the supervisory authority.

Moreover, according to article 34 of the GDPR, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. The latter communication of the breach to the data subject is irrespective of the aforementioned notification of the breach to the supervisory authority (which shall take place even when the risk cannot be considered as 'high'). The communication to the data subject shall take place, as much as possible, in an appropriate and effective way, in the form of personalized information rather than a general communication.

It should be noted that in any case, the supervisory authority can order the controller to communicate a personal data breach to the data subject (article 58 par 2 (e) of the GDPR).

The data controller should proceed with the notification through the portal of the HDPA designed for this purpose, by filling the appropriate form.

Following the assessment of the data controller that a notification before the authority is not required, the incident should be in any case documented internally on an appropriate manner in order for the authority to verify compliance with the provisions of the GDPR.

It is worth noted that other kind of non-compulsory notifications of incidents -meaning any event having an actual adverse effect on the security of network and information systems- affecting their business continuity with regards to the services provided are also stipulated in Law 4577/2018, implementing Directive 2016/1148 (NIS) on a high level of security of network and information systems under circumstances.

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with cybercrime, such as in the context of ransom payments following a ransomware attack?

Cybercrime cases are handled on a case-by-case basis by the competent state authorities, and in particular the Cyber Crime Division of Hellenic Police, while the directions of the competent administrative authorities are tailored to the specific characteristics of each case.

At national level there is no specific law dealing exclusively with cybercrime issues.

At legislative level there are various provisions of Greek criminal law that define specific forms of computer crime, such as Articles 386A of the Greek Penal Code regulating computer fraud, 370B of the Greek Penal Code on unlawful access to an information system or data – illegal copy of data, 370C of the Greek Criminal Code related to hacking. To the extent that these crimes are committed online – and as such falling under the definition of cybercrime – these articles are applicable in specific cases. Besides, some of them were updated recently through Law no. 5002/2022, which also created a provision for prohibiting the circulation of software, monitoring devices, and other data (art. 370F of the Greek Penal Code).

In addition, Law 4411/2016 ratified the Council of Europe Convention on Cybercrime and its Additional Protocol on the criminalization of acts of a racist and xenophobic nature committed through computer systems. Furthermore, the same law transposes, at national level, Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222 /JHA.

Last but not least, in case of a cybersecurity incident in critical infrastructure in the sense of Law no. 4577/2018, which implemented Directive 2016/1148/EU, Ministerial Decree No. 1027/2019 provides for the criteria for defining an event as a serious disruption to operators of essential services and the obligation to notify the competent Computer Security Incident Response Team (CSIRT) and the National Cyber Security Authority, without undue delay, in case of a cybersecurity incident.

38. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

As regards the public sector, Law no. 4577/2018, which implemented Directive 2016/1148/EU, provided for the

creation of the General Directorate of Cybersecurity, which is part of the General Secretariat of Telecommunications & Posts of the Ministry of Digital Governance. The Directorate has the responsibility to prepare the National Cybersecurity Strategy, wherein are defined the strategic objectives, priorities, as well as policy and regulatory measures, with the aim of ensuring a high level of security for telecommunications and information technology systems. Besides it is responsible for drafting the ICT security policy for the public sector and promoting its implementation, defining any security requirements and rules, as an integral part of every public ICT project even during the stage of development, cooperating with the competent Independent and Regulatory Authorities, ENISA and academic bodies, and coordinates training and awareness actions for the staff that manages and supports critical national systems and infrastructures.

Besides, under Law no. 5002/2022, a Coordinating Committee for Cybersecurity issues was established, which will act as the coordinating body between the General Directorate of Cybersecurity, the national CSIRT, the Directorate of Cyberspace of the Hellenic National Security Service, and the Hellenic Police. Its mission is to plan, monitor, coordinate actions, intervene in issues related to cybersecurity from the stage of prevention to the stage of effectively dealing with cyberattacks, and to minimize the effects of cyber threats.

In any case, cybersecurity issues are included in the responsibilities of different regulatory authorities such as the Hellenic Authority for Communication Security and Privacy, and the Hellenic Data Protection Authority.

At European level, in the field of information security, the European Network and Information Security Agency (Enisa) plays an important role. Regulation (EU) 2019/881 entrusts Enisa with critical tasks for the purpose of achieving a high level of cybersecurity throughout the Union, including actively supporting Member States, Union institutions, bodies and agencies in improving cybersecurity. Enisa shall act as a reference point for advice and expertise on cybersecurity for Union institutions, bodies, offices and agencies as well as for other relevant Union stakeholders.

39. Do the data protection laws in your jurisdiction provide individual data privacy rights, 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, any exceptions and any other relevant details.

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 is 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, 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.

40. Are individual data privacy rights exercisable through the judicial system, enforced by a regulator, or both?

Data subjects are entitled to exercise their rights before the data controllers, and they are also entitled to lodge complaints before the HDPA in case a violation takes place. This can further trigger the investigative powers of the Authority -which also acts ex officio- and can consequently lead to the imposition of fines on data controllers or their representatives, along with further administrative sanctions. Violation of respective obligations arising from the existing framework may also entail further criminal sanctions. Additionally, a violation of the framework as 'ratified' by a fine imposed by the competent Authority, may further lead to actions for damages before the competent courts.

41. 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 a 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.

42. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual damage to have been sustained, or is 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.

43. How are data protection laws in your jurisdiction 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.

44. 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.

45. 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.

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.

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.

46. Can controllers operating in your jurisdiction appeal to the courts against orders of the regulators?

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.

47. Are there any identifiable trends 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 is the creation of a cooperation and exchange of views platform whereas Data Protection Officers, other professionals with relevant practice area 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 sectors 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.

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

It is expected on a European level that the E-Privacy Regulation could enter into force in 2024.

While there aren't currently specific proposals for reforming the core data protection legislation in Greece, there are ongoing developments that might indirectly impact data protection such as:

The implementation of the NIS 2 Directive – Greece is working on incorporating the NIS 2 Directive (EU Directive 2022/2555) into its national legislation. This directive strengthens cybersecurity requirements for certain sectors, which can have a knock-on effect on data protection practices.

The upcoming EU AI Act which will set the standards for regulating high-risk AI applications.

Contributors

Dr. Themistoklis Giannakopoulos
Partner, Head of TMT, Antitrust, Competition and Regulatory Practice
themistoklis.giannakopoulos@gr.andersenlegal.com

Nicholas Zelios
Senior Associate
nikos.zelios@gr.andersenlegal.com

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