COUNTRY COMPARATIVE GUIDES 2021

The Legal 500 Country Comparative Guides

Greece

DATA PROTECTION & CYBER SECURITY

Contributing firm

Andersen Legal – Pistiolis – Triantafyllos & Associates Law Firm

Dr. Themistoklis Giannakopoulos

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

Kleio Kondi

Associate | kleio.kondi@andersenlegal.gr

Simeon Kretsis

Associate | simeon.kretsis@andersenlegal.gr

Nikos Zelios

Associate | nikos.zelios@andersenlegal.gr

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

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

GREECE
DATA PROTECTION & CYBER SECURITY

1. Please provide an overview of the legal and regulatory framework governing privacy 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It is noted that, pursuant to Article 84 of Law 4624/2019, a significant number of provisions of Law 2472/1997 are repealed while its provisions referred to in that article are retained.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.

Recently, the Hellenic Data Protection Authority has 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.

2. Are there any registration or licensing requirements for entities covered by these 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».*

3. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the 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.

4. What are the principles related to, the general processing of personal data or PII?

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.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII and, if so, are there are rules relating to the form, content and administration of such consent?

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.

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. At the same time, in case of electronic consent for sending emails, the controller shall follow specific procedures to confirm the subject's consent, such as the consent procedure with additional information and the double opt-in, as detailed below.

Furthermore, the right of a data subject to opt-out from unsolicited calls with human intervention is safeguarded, provided that the subscriber has notified the respective provider with his intention not to receive such calls. Provided that such notification has not taken place, providers can make unsolicited calls with human intervention, however the right to object is always possible during any received call.

6. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

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 the 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, archiving 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 defined by the GDPR.

Furthermore, paragraph 3 of the abovementioned article 22 provide 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.

7. How do the laws in your jurisdiction address children's personal data or PII?

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 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 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.

8. Does the law include any derogations, exclusions or limitations other than those already described? 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.

Finally, 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 are still subject to EU data protection laws.

9. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

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.

10. Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

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.

11. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

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.

12. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in 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.

13. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) 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.

14. Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice requirements (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 checked 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 has pointed out in practice that websites are subject to compliance with the information obligation towards the data subjects.

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, 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 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.

15. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (E.g. are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

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.

16. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g. due diligence or privacy and security assessments)?

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.

17. Please describe any restrictions on monitoring or profiling in your jurisdiction including the use of tracking technologies such as cookies. How are these terms defined and what restrictions 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 allowed only 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). For more details, the HDPA issued in 2020 guidelines and recommendations setting out its views of best practices

regarding the installation of cookies and the required user's consent.

18. Please describe any laws in your jurisdiction addressing email communication or direct marketing. How are these terms defined and what restrictions are imposed, if any?

Marketing purposes justify processing of personal data - in principle- on the basis of data subject's consent. According to Law 3471/2006, as further explained in Directive 2/2011 of the HDPA and by way of a derogation, e-mail details which were lawfully obtained within the context of products or services sales or any other transaction, can be used for direct marketing of similar products or services of the supplier or in order to serve similar purposes, even when the recipient of such e-mail has not previously provided one's consent, under the condition that it is provided to the latter in an explicit and distinct way the possibility to easily opt-out, free of charge to the collection and use of one's details upon the collection of the data and in any other message received, in case where the user had not initially disagreed to such use.

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.

19. Please describe any laws in your jurisdiction addressing biometrics, such as facial recognition. How are these 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, as discussed in Question 6 above.

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, which is the new national law laying down implementing measures for the General Data Protection Regulation at national level, does not contain any specific provisions regarding the processing of biometric data.

In addition, prior to the implementation of the GDPR, the HDPA issued a number of decisions regulating specific issues of biometric data processing, the following decisions are illustrative:

- 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'.

Specifically, on the issue of processing biometric data at work, HDPA in Directive 115/2001 states that the collection and processing of personal data of employees for purposes that do not directly or indirectly affect the

employment relationship is prohibited from the principle of purpose. 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.

20. Is the transfer of personal data or PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does cross-border transfer of personal data or PII require notification to or authorization form 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 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.

Under the previous regime a notification of the transfers based on a Commission Adequacy Decision or Standard Contractual Clauses was required before the HDPA and for the BCRs a national license was required to be issued. 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 in their current form without prejudice to any future update, they may be subject to.

Law 4624/2019 only comments on international transfers within the context of Directive's 2016/680 implementation with regard to 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 as the case may be.

21. What security obligations are imposed on personal data or PII owners/controllers and on 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 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 choice 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 individual 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.

22. Do the laws in your jurisdiction address security breaches and, if so, how does the law define "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.

23. Does your jurisdiction impose specific security requirements on certain sectors or industries (e.g. telecoms, infrastructure)?

The issue of information security is regulated by several provisions both at 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 who can ensure a strong level of security which is in line with the requirements set by the GDPR.

It is noted that at 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 national law 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.

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

24. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?

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 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).

Finally, any company can download the official notification form from the website of the HDPA, which shall be completed and sent to it in the case of a personal data breach.

25. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?

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 in an online environment – and as such falling under the definition of cybercrime – these articles are applicable in specific cases.

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.

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

At national level there is no separate authority that has a regulatory role. Moreover, even at European level, there does not seem to be a relevant model.

In Greece 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.

However, a crucial role at European level in the field of information security is played by the European Network and Information Security Agency (Enisa). Regulation (EU) 2019/881 entrusts Enisa with critical tasks for the purpose of achieving a high level of cybersecurity throughout the Union, including by 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.

27. Do the 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 the rights, how they are exercised, what exceptions exist 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.

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 is fifteen (15) working 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. In addition, in the course of 2020, the HDPA issued guidelines regarding the right to be informed about the use of CCTV, and also updated the templates of informative CCTV signs.

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 announcement towards the data subjects in the case of a data breach is foreseen where information due to their nature or the compelling legitimate interests of a third party should remain confidential. As already mentioned, the HDPA has commented that these additional restrictions are not duly specified as required by the GDPR. Therefore, it will assess within the context of exercising its powers whether such restrictions comply with the GDPR and the existing legal framework arising from the European Convention of Human Rights and the Charter of Fundamental Rights of the European Union.

28. Are individual data privacy rights exercisable through the judicial system or 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.

29. Does the law in your jurisdiction provide for a private right of action and, if so, in 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 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.

30. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?

Under Law 3471/2006 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. This was recently confirmed in the Case 415/2019 issued by the District Court of Athens, following the beginning of the implementation of the GDPR (relating however to an unsolicited call made before the GDPR starts applying), where the Court 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 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.

31. How are the laws governing privacy and data protection 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.

32. What is the range of fines and penalties for violation of these laws?

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.

33. Can personal data or PII owners/controller 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.

Contributors

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

Kleio Kondi
Associate
kleio.kondi@andersenlegal.gr

Simeon Kretsis
Associate
simeon.kretsis@andersenlegal.gr

Nikos Zelios
Associate
nikos.zelios@andersenlegal.gr