Global Data and Cyber Handbook - Greece

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# What's new?

## Recently Updated Topics

Main changes/additions made due to the expansion of the Survey to cover also issues referring to cybersecurity and artificial intelligence:

i. Among the cybersecurity laws and regulations the following have been added:

**Law 5160/2024** incorporating into Greek legislation Directive (EU) 2022/2555 (“**NIS2**”) of the European Parliament and of the Council of 14 December 2022 concerning measures to achieve a high common level of cybersecurity across the Union, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (“**NIS**”);

**Law 5099/2024** on adoption of measures for the implementation of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the single market for digital services (“**Digital Services Act**”);

**Law 5086/2024** on the establishment of National Cybersecurity Authority.

**Law 4537/2018** incorporating into Greek legislation Directive (EU) 2015/2366 on payment services in the internal market (“**PSD2 Directive**”)

ii. **Law 4727/2020** on Digital Governance incorporating into Greek legislation Directive (EU) 2016/2102 and Directive (EU) 2019/1024 – Electronic Communications incorporating into Greek legislation Directive (EU) 2018/1972, has been added in the new section on laws and regulations relating to non-personal data.

# Key Data & Cyber Contacts

## Contacts

The content for the Greece chapter has been prepared by the contact listed above from PPT Legal.

# Key Data & Cybersecurity Laws

## How are data and cybersecurity laws/regulations implemented?

*Last review date: 19 December 2024*

☒ omnibus – all personal data

☒ sector-specific

Law 3471/2006 governs the Electronic communications sector

## What are the key data privacy laws and regulations?

*Last review date: 19 December 2024*

*Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu) *for detailed information regarding EU-wide legislation.*

[EU General Data Protection Regulation](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679) ("**GDPR**")

Law 4624/2019 on "Hellenic Data Protection Authority ("**HDPA**"), measures for implementing GDPR and transposition of Directive (EU) 2016/680 and other provisions"

Law 3471/2006 on "protection of personal data and privacy in the electronic communications sector" [incorporation of Directive (EU) 2002/58]

## What are the key cybersecurity laws and regulations?

*Last review date: 19 December 2024*

*Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu) *for detailed information regarding EU-wide legislation.*

**Law 5160/2024** incorporating into Greek legislation Directive (EU) 2022/2555 (“**NIS2**”) of the European Parliament and of the Council of 14 December 2022 concerning measures to achieve a high common level of cybersecurity across the Union, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (“**NIS**”);

**Law 5099/2024** on adoption of measures for the implementation of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the single market for digital services (“**Digital Services Act**” or “**DSA**”); The National Telecommunications and Post Commission (EETT) is the National Digital Services Coordinator and is responsible for supervising and checking compliance with the rules of the DSA in Greece and the Hellenic Data Protection Authority (HDPA) has been designated as competent authority for the supervision of intermediary service providers and the enforcement of point d of paragraph 1 & paragraph 3 of article 26 of the DSA (on advertising on online platforms) and Article 28 of the DSA (on online protection of minors).

**Law 5086/2024** on the establishment of National Cybersecurity Authority.

Law 5002/2022 on "communications de-privacy process, cyber security and protection of citizens’ personal data", whereby provisions of Law 4624/2019 and Law 4577/2018 are amended;

Law 4961/2022 on “emerging information & communication technologies, reinforcement of digital governance and other provisions”.

**Law 4537/2018** incorporating into Greek legislation Directive (EU) 2015/2366 on payment services in the internal market (“**PSD2 Directive**”)

## What are the key laws and regulations relating to non-personal data?

*Last review date: 19 December 2024*

Law 4727/2020 on Digital Governance incorporating into Greek legislation Directive (EU) 2016/2102 and Directive (EU) 2019/1024– Electronic Communications incorporating into Greek legislation Directive (EU) 2018/1972.

## Are new or material changes to those key data and cybersecurity laws anticipated in the near future?

*Last review date: 19 December 2024*

**National (Greece) anticipated developments.**

Nothing has been announced in this respect.

# Regulators, Enforcement Priorities and Penalties

## Who are the main data privacy, non-personal data and/or cybersecurity regulator(s) in the jurisdiction?

*Last review date: 19 December 2024*

Greece has one data protection authority: The **Hellenic Data Protection Authority** ("[**HDPA**](http://www.dpa.gr/)"). According to article 5 of Law 5099/2024 on adoption of measures for the implementation of Regulation (EU) 2022/2065 (DSA), HDPA is responsible for the supervision of intermediary service providers and the enforcement of point (d) paragraphs 1 and 3 of Article 26 (on informing users how advertisements are displayed and targeted) and paragraph 1 of Article 28 (on the protection of personal data of minors) of the DSA.

Τhe **Greek Authority for Communication, Security and Privacy** ("**A.D.A.E**") is the Regulator designated by Law 3471/2006 (which incorporated EU Directive 2002/58 into the Greek legislation) to protect confidentiality of the communications as well as the security of networks and information systems and together with HDPA as the competent national authority to receive data breach notifications.

By virtue of Law 5086/2024, the **National Cybersecurity Authority** (**“NCA”**) has been established. According to article 4 of Law 5086/2024, the purpose of the NCA is to organize, coordinate, implement and control a comprehensive framework of strategies, measures and actions to achieve a high level of cybersecurity in Greece, at the level of prevention, protection, deterrence, detection, response, restoration and recovery from cyberattacks. According to article 17 of Law 5086/2024 the NCA has the power to impose sanctions in case of violations of the provisions of this law.

Pursuant to Law 5099/2024 on adoption of measures for the implementation of Regulation (EU) 2022/2065 (DSA), the **National Telecommunications and Post Commission** (**"EETT"**) is the National Digital Services Coordinator and is responsible for supervising and checking compliance with the rules of the DSA in Greece. EETT as the National Regulatory Authority regulates, supervises and monitors the electronic communications market, the use of the radio frequency spectrum and the postal market.

Pursuant to Law 4727/2020, the **General Secretariat for Public Administration Information Systems** of the Ministry of Digital Governance is responsible for the productive operation as well as the technical design of the Single Digital Portal of Public Administration (EPSP). The provision of digital public services and in particular the circulation of electronic documents, public or private, between public sector bodies on the one hand and natural persons or legal entities on the other hand, is carried out through the EPSP.

## How active is each of the regulator(s)?

*Last review date: 19 December 2024*

Moderately active

## What are each of the regulator's anticipated enforcement priorities for the next 12 months?

*Last review date: 19 December 2024*

The HPDA has imposed severe fines to data controllers for violation of principles of lawfulness and transparency, safety of processing and failure to satisfy data subjects’ rights.

It is anticipated that the HDPA will continue to put emphasis and impose penalties in cases of violations of the principles of lawfulness, transparency, integrity and confidentiality as well as cases of failure to satisfy data subjects’ rights.

EETT as Digital Services Coordinator and the HDPA, both as competent authorities pursuant to article 5 of Law 5099/2024 issued no. 1/2024 Joint Decision regulating issues relating to their cooperation in the context of the effective implementation of the DSA, in particular in the field of coordination of data and information collection and exchange, the use of information systems at national level and the procedure for receiving and transmitting complaints.

The main relevant responsibilities of the A.D.A.E. are to (i) conduct regular and special audits in public service facilities or private companies dealing with postal, telecommunication and other services; (ii) holding of hearings of electronic communications and postal services providers for the purpose of identifying possible violations of the applicable legislation to ensure confidentiality of communications; (iii) examining of complaints for violation of the confidentiality of telephone, internet and postal services communications and (iv) imposing administrative sanctions in cases of confidentiality of communication violations.

The purpose of the NCA is to organize, coordinate, implement and control a comprehensive framework of strategies, measures and actions to achieve a high level of cybersecurity in Greece, at the level of prevention, protection, deterrence, detection, response, restoration and recovery from cyberattacks.

## What trends are you seeing in regulatory investigations relating to data & cyber?

*Last review date: 19 December 2024*

Regulatory investigations or direct enforcement activity by data or cyber regulators are:

☒         Common

Class actions/group actions under data or cyber regulation are:

☒         Rare

## What are the potential penalties/remedies for non-compliance with the key data and cybersecurity laws in the jurisdiction?

*Last review date: 19 December 2024*

**There are:**

☒        administrative remedies from regulators and law enforcement

Law 4624/2019 leaves the administrative penalties provided in GDPR unchanged as regards private entities, which may amount to up to EUR 20 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Fines on public entities are limited by law up to EUR 10 million depending on the severity and duration of the violation.

☒        criminal penalties from regulators and law enforcement

According to Law 4624/2019 anyone who (a) interferes with a system of archiving personal data and with such action gains knowledge of such data, (b) copies, destructs, alters, collects, organizes, files, deletes, destroys and generally uses it illegally shall be punished with one year imprisonment. In case of special categories of data or data referring to criminal convictions or offenses, imprisonment of at least one year and a fine up to EUR 100,000 shall be imposed. If the offender intends for himself or for others to unlawfully gain economic benefit or to cause property damage and the total benefit thereof exceeds EUR 120,000, offender shall be punished with imprisonment up to ten years.

☒        private remedies  
Individuals may, for example:

file complaints with the data protection authorities

claim damages for material or non-material damages

☒        other

According to paragraph 4 of article 24 of Law 5160/2024 (incorporating article 32 of Directive 2022/2555 (NIS2) on supervisory and enforcement measures in relation to the basic entities:

*“4. The National Cybersecurity Authority, when exercising its supervisory duties in relation to key entities, has the following responsibilities:*

*(a) issue warnings or recommendations regarding violations of this Part by the entities concerned;*

*(b) issue binding instructions and guidelines, including on measures necessary to prevent or remedy an incident, and set deadlines for the implementation of such measures and for reporting on their implementation, or order the entities concerned to remedy identified deficiencies or violations of this Part;*

*(c) order the entities concerned to cease conduct that violates this Part and to refrain from repeating such conduct;*

*(d) order the entities concerned to ensure that cybersecurity risk management measures are in line with Article 15 or to fulfil the reporting obligations set out in Article 16, in a specific manner and within a specific period of time;*

*(e) instructs the relevant entities to inform natural or legal persons, in relation to whom they provide services or carry out activities that may be affected by a significant cyber threat, of the nature of the threat, as well as of any protective or remedial measures that such natural or legal persons may take to address that threat;*

*(f) instruct the entities concerned to implement the recommendations made as a result of a security audit within a reasonable period of time.*

*(g) appoint a competent supervisor with clearly defined tasks for a specified period of time, in order to supervise the compliance of the relevant entities with Articles 15 and 16,*

*(h) orders the relevant entities to make public information on violations of this part in a specific manner and procedure,*

*(i) impose administrative fines in accordance with article 26, in addition to the measures in paragraphs a) to h).”*

According to article 26 of Law 5160/2024 (incorporating articles 34 and 36 of Directive 2022/2555 (NIS2) on general conditions for the imposition of administrative fines to key and important entities - sanctions:

“*1. Supervisory or enforcement measures imposed on key or significant entities in relation to this Part shall be effective, proportionate and dissuasive, taking into account the circumstances of each individual case.*

*2. Sanctions against natural or legal persons for the violation of the provisions of this Part shall be imposed by a specifically reasoned decision of the Director of the National Cybersecurity Authority, which shall be issued after a hearing following their summons, in accordance with article 6 of the* ***Code of Administrative Procedure*** *(Law* ***2690/1999*** *, A` 45).*

*3. Decisions imposing fines and sanctions shall be notified to the interested parties and shall be posted, without delay, on the official website of the National Cybersecurity Authority. Decisions imposing fines and any other type of sanctions shall be appealed by means of an application for annulment to the competent Administrative Court of Appeal.*

*4. If a violation of Articles 15 or 16 is found, a fine of up to ten million (10,000,000) euros or up to two percent (2%) of the total worldwide annual turnover of the undertaking to which the significant entity belongs in the preceding financial year shall be imposed on the significant entities, whichever is higher.*

*5. If a breach of Articles 15 or 16 is found, a fine of up to seven million (7,000,000) euros or up to one point four percent (1.4%) of the total worldwide annual turnover of the undertaking to which the significant entity belongs in the preceding financial year shall be imposed on the significant entities, whichever is higher.*

*6. Administrative fines shall be imposed, in addition to the measures referred to in paragraphs a) to h) of paragraph 4 and paragraph 5 of article 24, as well as in paragraphs a) to g) of paragraph 4 of article 25, for the violation of paragraphs a) to h) of paragraph 4 and paragraph 5 of article 24, of a maximum amount of one million (1,000,000) euros, and for the violation of paragraphs a) to g) of paragraph 4 of article 25, of a maximum amount of seven hundred thousand (700,000) euros.*

*8. Without prejudice to the powers of the National Cybersecurity Authority in accordance with Articles 24 and 25, administrative fines shall be imposed on the entities referred to in point (f) of paragraph 2 of Article 3 that are subject to the obligations set out in this Part. Such fines may not be less than twenty thousand (20,000) euros and may not exceed five hundred thousand (500,000) euros.*

*9. If a violation is detected:*

*a) of paragraph 1 of article 14, a fine of a maximum amount of two hundred thousand (200,000) euros shall be imposed,*

*b) of paragraph 2 of article 14, a fine of a maximum of one hundred thousand (100,000) euros shall be imposed,*

*c) of article 19, a fine of a maximum of two hundred thousand (200,000) euros shall be imposed,*

*d) of article 20, a fine of a maximum of eight hundred thousand (800,000) euros shall be imposed,*

*e) of paragraph 3 of article 21, a fine of a maximum of one hundred thousand (100,000) euros shall be imposed,*

*f) of paragraphs 2 and 4 of article 24, a fine of a maximum of five hundred thousand (500,000) euros shall be imposed,*

*g) of paragraph 2 of article 25, a fine of a maximum of three hundred and fifty (350,000) euros shall be imposed, and*

*h) of paragraph 6 of article 15, a fine of a maximum of three hundred thousand (300,000) euros shall be imposed.”*

## If data subjects have private remedies, what form can these remedies take?

*Last review date: 19 December 2024*

☒         individual personal actions

☒         representative actions (e.g., brought by a consumer / data privacy body or the supervisory authority)

# Key Definitions

## Personal data

*Last review date: 19 December 2024*

"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.

## Sensitive/special personal data (including personal data subject to additional protections/ restrictions/breach notification obligations)

*Last review date: 19 December 2024*

**Sensitive data includes:**

☒         personal data revealing racial or ethnic origin  
☒         personal data revealing political opinions  
☒         personal data revealing religious or philosophical belief  
☒         personal data revealing trade union membership  
☒         genetic data  
☒         biometric data for the purpose of uniquely identifying a natural person  
☒         data concerning health/medical information  
☒         data concerning a natural person’s sex life or sexual orientation  
☒        personal data regarding an individual's criminal convictions or record

## Controller vs Processor

*Last review date: 19 December 2024*

**Do the privacy laws distinguish between controllers/owners and processors/agents? Whereby:**

the controller/owner is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

the processor/agent is natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Yes.

# Territorial Scope

## What is the territorial reach of the data privacy and cybersecurity laws?

*Last review date: 19 December 2024*

☒        applies to organizations located in the jurisdiction  
☒        applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction  
☒        applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction

# Legal Bases for Processing of Personal Data

## Is an identified legal basis required in order to collect or process non-sensitive personal data?

*Last review date: 19 December 2024*

Yes.

The following are potential legal bases for processing personal data:

☒        the data subject has provided consent to the processing for the identified purposes  
☒        the personal data is necessary to perform a contract with the data subject  
☒        the personal data is necessary to comply with a legal obligation  
☒        the personal data is necessary to protect the vital interests of a natural person  
☒        the personal data is necessary for a public interest  
☒        the personal data is necessary to fulfil a legitimate interest of the controller or third party (provided that the interest is not overridden by the data subject’s privacy interests and the data subject has not made use of his/her right to object)

## Is an identified legal basis required in order to collect or process sensitive personal data?

*Last review date: 19 December 2024*

Yes

The following are potential legal bases for processing sensitive personal data:

☒     the data subject has given consent to the processing, where consent is measured to a higher standard than for non-sensitive personal data (for example, additional requirement for consent to be "explicit")  
☒        processing is necessary for the purposes of 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  
☒        processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent  
☒        processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and further conditions  
☒        processing relates to personal data which are manifestly made public by the data subject  
☒        processing is necessary for the establishment, exercise or defense of legal claims  
☒        processing is necessary for reasons of substantial public interest  
☒        processing is necessary for the purposes of medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services  
☒        processing is necessary for reasons of public interest in the area of public health  
☒        processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes  
☒        other

Law 4624/2019 also allows processing of special categories of data by public entities for further purposes in cases where there are grounds of public interest, the necessity of preventing a significant threat to public safety and the necessity to take humanitarian measures.

## Are there special requirements that apply to the collection or processing of personal data from minors?

*Last review date: 19 December 2024*

Yes.

A minor within the meaning of data privacy laws is a person below the age of 15.

## In what circumstances do these special requirements apply?

*Last review date: 19 December  2024*

In the context of information society services only if processing is based on consent

## What are the special requirements that apply to collecting or processing personal data from minors?

*Last review date: 19 December 2024*

Consent must be given or authorized by the holder of parental responsibility over the child

# Information Requirements, Data Subject Rights, Accountability and Governance

## What information needs to be included in a privacy notice to data subjects?

*Last review date: 19 December 2024*

☒        the identity and the contact details of the controller and, where applicable, of the controller’s representative  
☒        the contact details of the data protection officer, where applicable  
☒        the purposes of the processing for which the personal data is intended  
☒        the legal basis for the processing  
☒        the categories of personal data concerned  
☒        the source from which the personal data originates, and if applicable, whether it came from publicly accessible sources  
☒        the legitimate interests pursued by the controller or by a third party if processing is based on the legitimate interests ground  
☒        the recipients or categories of recipients of the personal data, if any  
☒        information regarding data transfers to third countries, where applicable, and reference to appropriate or suitable safeguards and the means by which by to obtain a copy of them or where they have been made available  
☒        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 data subjects’ rights, such as the right to access, rectification, erasure, data portability, etc.  
☒        the existence of the right to withdraw consent if processing is based on consent  
☒        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  
☒        if applicable, information regarding automated decision making, including profiling

## Do data subjects have specific privacy rights that must be operationalized?

*Last review date: 19 December 2024*

Yes.

Data subjects have the following data privacy rights, although the specifics of the scope and conditions for each of these vary depending on the circumstances and local law:

☒         right to access the data subject’s own personal data  
☒         right to rectify/correct the data subject’s own personal data where inaccurate or incomplete  
☒         right to erasure of personal data  
☒         right to restrict data processing  
☒         right to data portability  
☒         right to object to the processing of personal data  
☒         right to withdraw consent  
☒         other

e.g., right to claim damages

## Are there accountability and governance requirements?

*Last review date: 19 December  2024*

Yes.

**There are accountability and governance requirements to:**

☒        take privacy by default and design measures for all processing of personal data  
☒        perform and document data protection impact assessments (DPIAs) for high-risk processing:  
The HDPA, with its decision no. 65/2018, published the list of the kind of processing operations which are subject to the requirement for a data protection impact assessment according to article 35 par. 4 of the GDPR (available in English [here](http://www.dpa.gr/portal/page?_pageid=33,223264&amp;amp;amp;_dad=portal&amp;amp;amp;_schema=PORTAL)).

☒        maintain a record of processing activities  
☒        implement appropriate measures to comply with data privacy and security  
☒        demonstrate compliance with data privacy and security  
☒        identify a specific individual as the data privacy contact for data subject or data protection authority inquiries  
☒        provide training to employees  
☒        audit or supervise data processors  
☒        appoint a local representative in the jurisdiction (if the controller or processor is not located in the jurisdiction)

# DPOs and Notification Requirements

## Is the concept of data protection officer (DPO) recognized in the jurisdiction?

*Last review date: 19 December 2024*

Yes.

## Are there circumstances in which it is mandatory to appoint a DPO or similar position?

Yes.

If yes, under what circumstances?

☒        the processing is carried out by a public authority or body, except for courts acting in their judicial capacity  
☒        the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale  
☒        the core activities of the controller or the processor consist of processing on a large scale of special categories of data

## Where a DPO is appointed, does the DPO have to meet specific requirements?

*Last review date: 19 December 2024*

Yes.

**If yes, what are these requirements?**

☒ legal qualifications / experience

☒ other professional qualifications / experience

☒ other

The DPO shall be designated on the basis of professional qualities and in particular having expert knowledge of data protection law and practices and the ability to fulfill the tasks referred to in article 39 of the GDPR.

## Are there obligations to notify, submit filings to, register with or obtain approval from local data protection authorities to collect and/or process personal data generally?

*Last review date: 19 December 2024*

No.

# Data Processors

## Are there obligations for controllers to establish controls with respect to data processors?

*Last review date: 19 December 2024*

Yes.

The obligations are as follows:

☒        controllers must conduct due conduct diligence on the processor to ensure it will provide appropriate security and processing of the personal data  
☒        controllers must only use processors subject to a written agreement that complies with specific requirements

## Are there any direct regulatory or statutory requirements on processors?

*Last review date: 19 December 2024*

Yes.

The following provisions apply directly to processors:

Art. 28, 29, 30 para. 2, 31, 32, 33 para. 2, 37 et seq., 44 et seq. GDPR.

# International Data Transfer

## Are there restrictions on the transfer of personal data to third countries?

*Last review date: 19 December 2024*

Yes.

Third country is not defined in the GDPR, but means countries (1) outside of the European Union, and (2) countries outside of the European Economic Area.

Transfers of personal data to third countries are permissible only, if there is a legal basis for the processing/transfer and one of the following applies:

☒        approved adequate/whitelisted jurisdictions  
☒        to holders of specific certifications or followers of specific code of conduct programs each approved by the relevant data protection and security authority  
☒        approved standard contractual clauses  
☒        binding corporate rules  
☒        derogations, such as consent, contract performance, necessity to establish, exercise or defend legal claims

***Please see separate question for information on data localization provisions that are not restricted to personal data.***

ad-hoc contracts approved by the data protection authority

# Cookies, Online Tracking and Direct Marketing

## Are there specific requirements for the use of cookies and other online tracking technologies?

*Last review date: 19 December 2024*

Yes

According to par. 5 of article 4 of Law 3471/2006:

*“5. Storing information or gaining access to already stored information in the terminal equipment of a subscriber or user is only permitted if the specific subscriber or user has given his consent after clear and extensive information. Subscriber or user consent may be given through appropriate settings in the web browser or through another application. The above does not prevent any technical storage or access, the sole purpose of which is to carry out the transmission of a communication via an electronic communications network or which is necessary for the provision of an information society service, which has been expressly requested by the user or the subscriber.”.*

In view of the above, the excluded cookies and related technologies are essentially those considered technically necessary to make the connection to the website or to provide the internet service.

## Are there specific requirements related to the use of personal data for direct marketing activities?

*Last review date: 19 December 2024*

Yes.

**☒   email marketing**

☒        prior opt-in consent  
☒        prior existing business relationship (and subject to other requirements) with opt-out consent

**☒   telephone marketing**

☒        prior opt-in consent  
☒        opt-out or implied consent

**☒   SMS/text message marketing**

☒        prior opt-in consent  
☒        prior existing business relationship (and subject to other requirements) with opt-out consent

**☒   postal marketing**

☒        prior opt-in consent  
☒        prior existing business relationship (and subject to other requirements) with opt-out consent

**☒   online behavioral advertising targeting//social media targeting/ad personalization marketing**

☒        prior opt-in consent  
☒        prior existing business relationship (and subject to other requirements) with opt-out consent

# Data Processing in the Employment Context

## Is an identified legal basis required in order to collect or process personal data or sensitive personal data in the employment context?

*Last review date: 19 December 2024*

Yes.

The potential legal bases for data processing in the employment context are:

The same as in a non-employment context.

## Can consent be validly obtained in the employment context?

*Last review date: 19 December 2024*

Yes, but this consent is typically more difficult to establish in an employment context (specify details below)

Yes, but care needs to be taken as, pursuant to recital 43, "consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller", which could be the case in the employment relationship.

Pursuant to Law 4624/2019 in cases where processing is performed on the legal basis of the employee's consent, the validity of consent is evaluated according to the circumstances of the specific employment contract and the conditions of consent in accordance with article 7 GDPR.

## Has the data privacy regulator issued guidance on use of artificial intelligence, automated decision making or profiling in an employment context – for example, relating to use in employee monitoring or hiring?

*Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu) *for detailed information regarding EU-wide legislation.*

No

No guidance on this specific issue has been produced at a national level.

See the separate section on artificial intelligence, automated decision making and profiling for general EU guidance.

# Artificial Intelligence, Profiling and Automated Decision Making

## Are there any restrictions or requirements related to creating profiles of data subjects or utilizing automated decision-making for decisions related to data subjects, including with respect to artificial intelligence?

*Last review date: 19 December 2024*

Yes.

The restrictions or requirements are as follows:

☒        qualified right not to be subject to a decision based solely on automated decision making, including profiling – for example, only applicable if the decision produces legal effects concerning them or similarly significantly affects them

☒        right to information / transparency requirement

☒        right to request human review of the automated decision making

☒        other

Par. 1 of article 52 of Law 4624/2019 in accordance to article 11 of EU Directive 2016/680 provides that:

*“1. It is prohibited to take a decision based solely on automated processing, including profiling, which produces adverse legal effects for the data subject or significantly affects him, unless expressly provided for by a statutory provision or Union law, which defines the appropriate guarantees for the rights and freedoms of the data subject and, as a minimum, includes arrangements guaranteeing the specific and indiscernible information of the data subject, the right to ensure human intervention on the part of the controller and the right of the data subject to formulate his views, to demand justification of the decision taken following said assessment and to challenge or request a review of the decision.”.*

## If such restrictions or requirements exist, are they subject to any exceptions?

*Last review date: 19 December 2024*

Yes.

As provided in article 22 of the GDPR, the exceptions are as follows:

If the decision:

is necessary for entering into, or performance of, a contract between the data subject and a data controller;

is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights/freedoms and legitimate interests; or

is based on the data subject's explicit consent.

## Has the data privacy regulator issued guidance on data privacy and artificial intelligence, automated decision-making or profiling?

*Last review date: 19 December 2024*

*Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu) *for detailed information regarding EU-wide legislation.*

No guidance on this has been produced at a national level.

## Has the data privacy regulator taken enforcement action in relation to artificial intelligence, including automated decision-making or profiling?

*Last review date: 19 December 2024*

No enforcement activity to date

## Do other (non-personal data or cybersecurity) laws or regulations impose restrictions on use of artificial intelligence, automated decision-making or profiling?

*Last review date: 19 December 2024*

*Please refer to the* [*EU Chapter*](https://resourcehub.bakermckenzie.com/en/en/resources/global-data-and-cyber-handbook/emea/eu) *for detailed information regarding EU-wide legislation.*

Yes, laws in force

Article 9 of Law 4961/2022, provides the following:

*“Obligation to inform about the use of artificial intelligence in the labor sector*

*1. Any private sector enterprise, as long as it uses an artificial intelligence system, which affects any decision-making process concerning employees or prospective employees and has an impact on their working conditions, selection, recruitment or evaluation, in any case before its first use, provides sufficient and clear information to every employee or prospective employee, which includes the parameters on which the decision is based, without prejudice to the cases that require prior information and consultation and ensures compliance with the principle of equal treatment and the fight against discrimination in employment and work due to gender, race, color, national or ethnic origin, genealogy, religious or other beliefs, disability or chronic condition, age, family or social status, sexual orientation, gender identity or characteristics.*

*2. The obligation of par. 1 also applies to digital platforms within the meaning of article 68 of Law 4808/2021 (A' 101), in terms of natural persons connected to them by contracts of dependent work or independent services or work.*

*3. The administrative and criminal sanctions of Articles 24 and 28, respectively, of Law 3996/2011 shall be imposed on the business that violates the obligation of paragraph 1. The competent authority for imposing the administrative sanctions of the first paragraph is the Labor Inspection Body (S.E.P.E.).*

*4. The obligations set by this article do not in any way affect the obligations set by article 22 of the GDPR for automated individual decision-making, including profiling.”.*

The European Parliament and the Council have reached a political agreement on the EU AI Act, which is now subject to formal approval by the European Parliament and the Council. The final text of the AI Act is currently not available but is expected early 2024.

The Digital Services Act (Regulation 2022/2065 of 19 October 2022 on a Single Market For Digital Services - “**DSA**”), which will be fully applicable as from 17 February 2024, sets forth specific restrictions with respect to certain uses of profiling. In particular, under Art. 26 (3) of the DSA, providers of online platforms may not present advertisements to recipients of the service based on profiling as defined in Art. 4 GDPR using special categories of personal data referred to in Art. 9 (1) GDPR. Furthermore, pursuant to Art. 28 (2) of the DSA, providers of online platforms may not present advertisements on their interface based on profiling (within the meaning of Art. 4 GDPR) using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor. Lastly, according to Art. 38 DSA, providers of very large online platforms and of very large online search engines that use recommender systems must provide at least one option for each of their recommender systems which is not based on profiling (within the meaning of Art. 4 GDPR).

It is also worth pointing out that according to Art. 15 of the Digital Markets Act (Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector), within 6 months after its designation, a gatekeeper must submit to the Commission an independently audited description of any techniques for profiling of consumers that the gatekeeper applies to or across its core platform services listed in the designation decision. The Commission will transmit that audited description to the European Data Protection Board.

# Data privacy and cybersecurity in a transactional context

## Has the data privacy authority issued any guidance on data privacy compliance in the context of transactional activity (including, but not limited to, share sales, asset sales, reorganizations or spinouts)?

*Last review date: 19 December 2024*

No

No guidance on this specific issue has been produced at a national or European level.

## In the context of an asset sale (the sale of a separate business unit as a going concern), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the assets that are the subject of the asset sale)?

*Last review date: 19 December 2024*

It depends (for example, on the way the asset sale is structured, and/or the assets being acquired)

## If so, how would any regulatory fines be calculated?

*Last review date: 19 December 2024*

Unclear

We have not been able to trace a publicly available decision issued by the HDPA in this respect.

## In the context of a share sale (where the acquiring entity acquires 100% of the shares of a target company), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the target company)?

*Last review date: 19 December 2024*

It depends (for example, on the way the share sale is structured)

## If so, how would any regulatory fines be calculated?

*Last review date: 19 December 2024*

Unclear

We have not been able to trace a publicly available decision issued by the HDPA in this respect.

# Security Requirements and Breach Notification

## Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last review date: 19 December 2024*

Yes.

☒         general obligation to take appropriate / reasonable technical, physical and/or organizational security measures  
☒         obligation to take specific security measures e.g., encryption

Not a strict legal requirement, but encryption is considered by the GDPR as an appropriate technical and organizational measure. In practice, the authorities expect encryption unless specific circumstances justify no encryption.

## Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last review date: 19 December 2024*

☒       public company obligations (e.g., duties to maintain sufficient information security measures or ensure operational resilience to cyberattacks?)

☒       network information security requirements (broader than telecommunications)

☒       health regulatory requirements

☒       financial services requirements

☒       telecommunication requirements

☒       providers of critical infrastructure

☒       digital or connected (IoT) products

☒       other

According to paragraph 1 of article 15 of Law 5160/2024 incorporating article 21 and paragraph 1 of article 24 of Directive 2022/2555 (NIS2):

“*1. Key and significant entities shall take appropriate and proportionate technical, operational and organizational measures to manage the risks to the security of network and information systems that they use for their activities or for the provision of their services and to prevent or minimize the impact of incidents on the recipients of their services or on other services and organizations. Taking into account the most up-to-date and, where appropriate, relevant national, European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems that is proportionate to the risk involved. When assessing the proportionality of those measures, account shall be taken of the entity's exposure to risks, the size of the entity, the likelihood of incidents occurring and their severity, including their social and economic impact.”*

## Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

☒      Data privacy

☒      Securities or public company

☒      network information security

☒      financial services

☒      telecommunications

## Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last review date: 19 December 2024*

Yes.

"Personal data breach" means 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.

## Controllers/Owners have to notify:

*Last review date: 19 December 2024*

☒   data protection authorities

in case of a personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons  
  
without undue delay and, where feasible, not later than 72 hours after having become aware of it

☒   affected individuals

without undue delay

According to para. 1 of article 34 of GDPR:

"*When the personal data breach is likely to result 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"*

if a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, unless any of the following conditions are met:

the controller has implemented technical and organizational protection measures and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption

the controller has taken subsequent measures that ensure that the high risk to the rights and freedoms of the data subjects is no longer likely to materialize

it would involve disproportionate effort

☒   other

There shall be public communication or similar measure whereby the data subjects are informed in an equally effective manner (instead of informing the data subjects) if the communication to the data subject would involve disproportionate effort.

Above is the exception provided in para. 3(c) of article 34 of GDPR, where there is no provision of either specific or general timeframe for breach notification.

## Processors/Agents have to notify:

*Last review date: 19 December 2024*

☒        controller/ owner

in case of a personal data breach irrespective of a risk to the rights and freedoms of the data subjects

without undue delay after becoming aware of it

## Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last review date: 19 December 2024*

☒        cybersecurity authorities  
☒        other

On 23 September 2020, the Greek Government published Law 4727/2020 on the incorporation in Greek legislation of EU Directives 2016/2102, 2019/1024 and 2018/1972 (**"EECC"**) and other provisions in the Issue of Government Gazette nr. 184/A/23.09.2020.

In particular article 40 of the EU Directive 2018/1972 has been incorporated in Greek legislation by article 148 of Law 4727/2020.

In particular, article 148 of Law 4727/2020 -which more or less constitutes translation in Greek of the relevant provisions of article 40 of the EU Directive EECC - provides with regard to the notification timeframe the following:

"*providers of public electronic communications networks or of publicly available electronic communications services* *notify without delay* *A.D.A.E. (*i.e. the Hellenic Authority for Communication Security & Privacy)*every security incident that has had a significant impact on the operation of networks and services".*

According to article 16 of Law 5160/2024 (incorporating article 23 of Directive 2022/2555 (NIS2) on incident reporting obligations:

“*1. Key and significant entities shall notify, without delay, the Computer Security Incident Response Team (***"CSIRT"***) of the National Cybersecurity Authority of any incident that has a significant impact on the provision of their services, in accordance with paragraph 3 (significant incident). Where appropriate, the entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that may adversely affect the provision of those services. Such entities shall, inter alia, report any information that allows the National Cybersecurity Authority to determine the cross-border implications of the incident. The simple act of notification does not entail liability of the notifying entity. In the event of a cross-border or cross-sectoral significant incident, the National Cybersecurity Authority shall provide, without delay, to the single points of contact referred to in paragraph 8 the relevant information notified to it in accordance with paragraph 4.*

*2. Key and significant entities shall, without delay, notify the relevant recipients of their services that may be affected by a significant cyber threat of measures or remedial actions that they can take to address that threat. The entities shall also inform those recipients of the significant cyber threat.*

*3. An incident is considered significant if:*

*a) has caused or may cause serious operational disruption of services or financial damage to the entity concerned,*

*b) has affected or may affect other natural or legal persons, causing significant material or non-material damage.*

*4. For the notification of par. 1, the relevant entities shall submit to the National Cybersecurity Authority:*

*a) without undue delay and in any event within twenty-four (24) hours of becoming aware of the significant incident, a warning, which, where appropriate, states whether there is a suspicion that the significant incident was caused by illegal or malicious actions or could have a cross-border impact.*

*b) without undue delay and in any case within seventy-two (72) hours from the moment they became aware of the significant incident, an incident notification, which, where applicable, updates the information referred to in point a) and, in addition, includes an initial assessment of the significant incident, including its severity and impact, as well as, if any, the indications of the breach,*

*c) upon request of the National Cybersecurity Authority, an interim report on relevant updates of the situation,*

*d) a final report no later than one (1) month after the submission of the incident notification in accordance with paragraph b).”*

# Data localization and regulation of non-personal data

## Are there data localization/data residency or other types of laws that may require the retention and storage of data in the local jurisdiction, or prohibit the transfer of data out of the jurisdiction?

*Last review date: 19 December 2024*

Yes.

Other laws that may require the retention and storage of personal data (including, for example, where such data is part of another type of record or dataset) in the local jurisdiction or otherwise prohibit the transfer or disclosure of the personal data outside of the local jurisdiction:

☒         tax or financial record laws

☒         employment laws

## Does law or regulation impose mandatory requirements to share or make accessible non-personal data?

*Last review date: 19 December 2024*

☒         Obligation for public sector organizations to share or make accessible non-personal data

☒         Obligation for private organizations to share or make accessible data generated by connected or "IoT" devices

***If so, please provide brief details of the relevant law or regulation.***

Paragraphs 1 and 2 of article 8 and article 10 of Law 5099/2024 on adoption of measures for the implementation of DAS (the Act) provide as follows:

Article 8 on the co-operation between the Digital Services Coordinator and competent authorities:

“*1. The Digital Services Coordinator and the competent authorities of Article 5 shall cooperate closely, provide mutual assistance and exchange in a direct and effective manner all information at their disposal for the implementation of the Act and this Law, within the deadlines set by the Act or this Law, otherwise within the deadline set by the party requesting cooperation, in order to comply with the deadlines set by the Act.*

*2. The Digital Services Coordinator and the competent authorities referred to in Article 5 may exchange and use data and information at their disposal, including personal data and information covered by business and professional secrecy, to the extent necessary for the performance of their tasks. In relation to the information exchanged, the receiving authority shall ensure the same level of confidentiality as the transmitting authority.”*

Article 10 on the co-operation of the Digital Services Coordinator with other authorities:

*“Public authorities, which are not included in the competent authorities of article 5, and in particular the Ministry of Development, shall actively cooperate with the Digital Services Coordinator for the fulfillment of the objectives of the Act and this law, concluding relevant cooperation agreements, when deemed necessary. In this context, they shall provide, upon request of the Digital Services Coordinator, their assistance, including information deemed necessary for the fulfillment of the objectives of the Act and this law, in particular for the management of complaints. The above authorities shall respond to written requests from the Digital Services Coordinator for the provision of information and any kind of assistance, within the deadline that he sets in his request, in order to comply with the deadlines set by the Act”.*

## What specific obligations do these data-sharing rules impose on private organizations?

*Last review date: 19 December 2024*

☒         Obligation to share data on request

☒         Obligation to (re)design products or services to facilitate data accessibility

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.