

## TABLE OF CONTENTS

### INTRODUCTION

#### + 1. GOVERNING TEXTS

1.1. Key acts, regulations, directives, bills

1.2. Guidelines

1.3. Case law

#### + 2. SCOPE OF APPLICATION

2.1. Personal scope

2.2. Territorial scope

2.3. Material scope

#### + 3. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY

3.1. Main regulator for data protection

3.2. Main powers, duties and responsibilities

### 4. KEY DEFINITIONS

#### + 5. LEGAL BASES

5.1. Consent

5.2. Contract with the data subject

5.3. Legal obligations

5.4. Interests of the data subject

5.5. Public interest

5.6. Legitimate interests of the data controller

5.7. Legal bases in other instances

### 6. PRINCIPLES

#### + 7. CONTROLLER AND PROCESSOR OBLIGATIONS

7.1. Data processing notification

7.2. Data transfers

You have **4 out of 5** free articles left for  
the month

Signup for a trial to access unlimited  
content.

**Start Trial**  


- 7.3. Data processing records
- 7.4. Data protection impact assessment
- 7.5. Data protection officer appointment
- 7.6. Data breach notification
- 7.7. Data retention
- 7.8. Children's data
- 7.9. Special categories of personal data
- 7.10. Controller and processor contracts
- + 8. DATA SUBJECT RIGHTS
  - 8.1. Right to be informed
  - 8.2. Right to access
  - 8.3. Right to rectification
  - 8.4. Right to erasure
  - 8.5. Right to object/opt-out
  - 8.6. Right to data portability
  - 8.7. Right not to be subject to automated decision-making
  - 8.8. Other rights
- + 9. PENALTIES
  - 9.1 Enforcement decisions

## December 2021

---

## INTRODUCTION

In Greece, the protection of a person's personal data against any collection, processing, and use, has been constitutionally safeguarded (see Article 9A of the Constitution of Greece, as revised in 2001 (only available in Greek [here](#)). Pursuant to said provision, an independent authority shall ensure the protection of personal data.

The [Hellenic Data Protection Authority](#) ('HDPA') is the national regulatory authority and has the competency to apply the data protection rules in the Greek territory. The main legal framework consists

You have 4 out of 5 free articles left for the month. Sign up for a trial to access unlimited content. [Start Trial](#) 

the national implementation law. In addition, the HDPa also follows EU guidance (e.g. guidelines and recommendations by the [European Data Protection Board](#) ('EDPB')) when exercising its powers.

This year, the HDPa continued to provide guidance in relation to the challenges faced in Greece also in the data privacy field in the context of the measures adopted for the protection against the Covid-19 pandemic. Further to its last year's guidelines on the subject matter (see Guidelines 3/2020 on the processing of personal data in the context of the management of Covid-19 (only available in Greek [here](#)) and Guidelines 2/2020 on the adoption of security measures in the context of the teleworking (only available in Greek [here](#))), the HDPa issued in August 2021 its Guidelines on the application of data privacy rules in the context of teleworking (only available in Greek [here](#)), having regard to the intensity and extent of remote working due to the pandemic and the risks posed by the use of information and communication technologies for the rights of data subjects and security of infrastructure. The HDPa also issued in May 2021 a notice on the processing of personal data in the context of conducting COVID-19 self-tests, by means of which it highlighted the importance of the accountability principle under the GDPR and directed data subjects directly to data controllers for the exercise of their rights (only available in Greek [here](#)). In the context of this notice, the HDPa clarified that the mere demonstration of the negative results of the self-diagnostic tests, provided that these are not included in a filing system, nor are subjected to automated processing, does not qualify in the first place as processing of personal data falling within the scope of Article 2 of the GDPR and the Greek data privacy rules.

---

## 1. GOVERNING TEXTS

### 1.1. Key acts, regulations, directives, bills

Law No. 4624/2019 on the Personal Data Protection Authority, Implementing the General Data Protection Regulation (Regulation (EU) 2016/679) and Transposing into National Law Data Protection Directive with Respect to Law Enforcement (Directive (EU) 2016/680) and Other Provisions (only available in Greek [here](#)) ('the Data Protection Law') which implements certain provisions of the GDPR, is the basic national legal framework on personal data protection in Greece along with the GDPR.

Apart from the Data Protection Law, [Law 3471/2006 on the protection of personal data and privacy in the electronic communications sector](#) ('the Electronic Communications Law'), as in force, incorporates the [Directive on Privacy and Electronic Communications \(2002/58/EC\) \(as amended\)](#) ('the e-Privacy Directive') and provides specific rules on the protection of personal data in the field of elec-

You have 4 out of 5 free articles left for the month

Signup for a trial to access unlimited content.

**Start Trial** 

## 1.2. Guidelines


The HDPa has released guidance addressed to data controllers concerning different topics of the GDPR, such as:

- principles relating to the processing of personal data, only available in Greek [here](#), including on the conditions for the lawful processing, only available in Greek [here](#), and conditions for consent, only available in Greek [here](#);
- guide to with the general obligations under the GDPR (only available in Greek [here](#));
- records of processing activities and relevant templates for both data controllers and data processors (both only available in Greek [here](#));
- security of processing (only available in Greek [here](#));
- personal data breach notification (only available in Greek [here](#));
- personal data breach notification form to be submitted to the HDPa in an encrypted form (only available in Greek [here](#));
- codes of conduct (only available in Greek [here](#));
- obligations relevant to electronic communications (only available in Greek [here](#));
- data protection officer ('DPO') (only available in Greek [here](#));
- DPO appointment notification form to be filled in and submitted electronically to the HDPa (only available in Greek [here](#));
- designation of a lead authority (only available in Greek [here](#));
- certification (only available in Greek [here](#));
- Data Protection by Design and by Default (only available in Greek [here](#));
- accountability principle (only available in Greek [here](#));
- transfers of personal data (only available in Greek [here](#));
- data protection impact assessment ('DPIA') (only available in Greek [here](#));
- HDPa list of processing operations requiring a DPIA (only available in Greek [here](#));
- prior consultation (only available in Greek [here](#));
- 'registry of Article 13' of the authority (only available in Greek [here](#)); and
- the CCTV templates.

The HDPa also refers to the various guidelines that were issued by the EDPB, which replaced the [Article 29 Working Party](#).

## 1.3. Case law

The HDPa's case law concerning the GDPR is steadily developing with respect to different topics, including the following:

You have **4 out of 5** free articles left for the month. Signup for a trial to access unlimited content. **Start Trial** 

- principles relating to the processing of employees' data, namely through CCTV system (see HDPa Decision 12/2021 [here](#), HDPa Decision 23/2021 [here](#), HDPa Decision 39/2021 [here](#), and HDPa Decision 41/2021 [here](#), all only available in Greek);
- processing of insured persons personal data by insurance company (see HDPa Decision 5/2021, only available in Greek [here](#));
- infringement of Article 28 of the Data Protection Law (on freedom of expression) and Article 5 (1)(c) of the GDPR (see HDPa Decision 15/ 2021 [here](#), and HDPa Decision 25/2021 [here](#), both only available in Greek);
- non-compliance with the exercise of data subject's rights, namely the right to access, the right to erasure, and the right to object (see HDPa Decision 13/2021 [here](#), HDPa Decision 17/2021 [here](#), HDPa Decision 20/2021 [here](#), HDPa Decision 26/2021 [here](#), HDPa Decision 29/2021 [here](#), HDPa Decision 36/2021 [here](#), and HDPa Decision 37/2021 [here](#), all only available in Greek);
- unsolicited communication for political purposes (through electronic means, such as SMS, email etc.) (see HDPa Decision 3/2021 [here](#), HDPa Decision 4/2021 [here](#), HDPa Decision 7/2021 [here](#), HDPa Decision 8/2021 [here](#), HDPa Decision 9/2021 [here](#), HDPa Decision 16/2021 [here](#), HDPa Decision 18/2021 [here](#), and HDPa Decision 19/2021 [here](#), all only available in Greek; and
- deletion from recipients lists pursuant to the Electronic Communications Law (see HDPa Decision 11/2021, only available in Greek [here](#)).

---

## 2. SCOPE OF APPLICATION

### 2.1. Personal scope

No national law variations exist.

### 2.2. Territorial scope

The Data Protection Law has a similar material scope to the GDPR but distinguishes between public bodies and private entities that process personal data (Article 2 of the Data Protection Law).

### 2.3. Material scope

The provisions of the Data Protection Law apply to public bodies. With regard to private bodies,

these apply, provided that (Article 3 of the Data Protection Law):

You have 4 out of 5 free articles left for the month. Sign up for a trial to access unlimited content.

**Start Trial**  


- the data controller or data processor is processing personal data within the Greek territory;
- the personal data is subject to processing in the context of the activities of an establishment of the data controller or the data processor within the Greek Territory; or
- the data controller or data processor falls within the GDPR scope even if not established in an EU Member State or another country of the European Economic Area ('EEA').

## 3. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY


### 3.1. Main regulator for data protection

The HDPa is responsible for monitoring the implementation of the GDPR provisions, the Data Protection Law and other provisions related to the protection of persons against the processing of personal data in the Greek territory.

### 3.2. Main powers, duties and responsibilities

Besides its powers under Article 58 of the GDPR, the HDPa has been provided with the following investigative and corrective powers under Article 15 of the Data Protection Law:

- to carry out, ex officio or following a complaint, investigations, and audits over compliance with the provisions of the Data Protection Law in the context of which technological infrastructure and other, automated or not means, that support the processing of personal data are also investigated;
- to address warnings to the data controller or data processor that intended processing operations are likely to infringe provisions of the Data Protection Law;
- to order the data controller or data processor to bring processing operations into compliance with the provisions of the Data Protection Law, in a specified manner and within a specified period, particularly by means of an order for the rectification or erasure of personal data;
- to order and impose a temporary or definitive limitation and/or ban on the processing of personal data;
- to order and impose the delivery to the authority of documents, filing systems, equipment, or processing means of personal data and their content;
- to seize any documents, information, filing systems of any equipment and means of a personal data breach, including their content, that comes to its attention when exercising its

You have 4 out of 5 free articles left for the month. Sign up for a trial to access unlimited content. [Start Trial](#) 

- to order the data controller or data processor to interrupt the processing of personal data, to return or 'freeze' the relevant data, or to destroy the filing system or relevant data;
- to impose administrative sanctions under Article 83 of the GDPR and Article 39 of the Data Protection Law;
- to impose administrative sanctions under Article 82 of the GDPR;
- to issue a provisional order for the immediate, whole, or partial, temporary limitation of the processing or of the file operation until issuance of a final decision; and
- to issue administrative regulatory acts in order to regulate specific, technical, and detailed matters.

---

## 4. KEY DEFINITIONS

**Data controller:** There is no national variation to this definition.

**Data processor:** There is no national variation to this definition.

**Personal data:** There is no national variation to this definition.

**Sensitive data:** There is no national variation to this definition.

**Health data:** There is no national variation to this definition.

**Biometric data:** There is no national variation to this definition.

**Pseudonymisation:** There is no national variation to this definition.

It is noted that, although no national law variations exist, distinction is made under the Data Protection Law between public and private entities when acting as controllers, as different treatment applies with regard to the restrictions imposed on personal data processing depending on the type of organisation.

**Public bodies:** the public authorities, the independent and regulatory administrative authorities, the public entities (i.e., legal persons of public law), local authorities (municipalities etc.) of first and second degree and their legal entities and their undertakings, the state and public undertakings and public bodies, the legal entities of private law which belong to the state or which are subsidised by 50% at least of their annual budget by the state or their management is appointed by the state.

You have **4 out of 5** free articles left for  
the month

Signup for a trial to access unlimited  
content.

**Start Trial**  


**Private bodies:** the natural or legal person or association of persons without a legal entity, that does not fall within the notion of 'public body'.

---

## 5. LEGAL BASES

### 5.1. Consent

The GDPR allows for EU Member States to lower child's consent age below 16 for online service providers offering services directly to children. The Data Protection Law lowers the age of child consent to 15 years (see Article 21 of the Data Protection Law).

### 5.2. Contract with the data subject

No national law variations exist.

### 5.3. Legal obligations

No national law variations exist.

### 5.4. Interests of the data subject

No national law variations exist.

### 5.5. Public interest

No national law variations exist.

### 5.6. Legitimate interests of the data controller

No national law variations exist.

### 5.7. Legal bases in other instances

Not applicable.

For direct marketing cases, the HDPAL would apply the provisions under the Electronic Communications Law.

You have **4 out of 5** free articles left for **Processing of employee data** the month

Signup for a trial to access unlimited content.

**Start Trial** 



Article 27 of the Data Protection Law sets out provisions that apply to the processing of personal data of employees in the context of employment.

In particular, it is specified that the provisions under the Data Protection Law apply to all employees, regardless of the specific type of the employment relationship, of the validity of the contract, and irrespective of whether processing involves applicants' or former employees' personal data.

Further, the Data Protection Law provides that employees' personal data may be subject to processing for the purposes of the employment contract, so long as this is strictly necessary for the decision of conclusion of the employment contract or following the employment contract's conclusion for its performance (Article 27(1) of the Data Protection Law).

According to HDPa Opinion (see pages 16-19 of the HDPa Opinion), to the extent that Article 27(1) of the Data Protection Law introduces a sole legal basis of processing in the employment context, in which all legal bases of Article 6(1) of the GDPR are merged, such provision is in contradiction to the provisions of Article 88(1) of the GDPR allowing for the provision of more specific national rules and not for the creation of a new legal basis or for the exclusion of legal bases under the GDPR. Hence, the HDPa has considered that Article 27(1) of Data Protection Law is not in line with the GDPR.

By way of exception, the Data Protection Law provides that the processing of employees' personal data may be based, in exceptional circumstances, on consent, so long as such consent has been the result of free choice, taking into account in particular:

- the existing dependence under the employment contract; and
- the circumstances under which consent was given.

Under the Data Protection Law, consent is provided either in written form or electronically and must be clearly distinguished from the employment contract. The employer should inform the employee either in written form or electronically of the processing purpose and of employees' right to withdraw their consent in accordance with Article 7(3) of the GDPR.

Notwithstanding specific provisions under Article 9(1) of the GDPR, the processing of special categories of personal data for the purposes of the employment contract is permitted provided it is necessary for the exercise of the rights, or the carrying out of the lawful obligations arising from employment law, as well as social security and social protection law, and there is no reason to consider that data subjects' legitimate interests prevail.

You have **4 out of 5** free articles left for the month

Signup for a trial to access unlimited content.

**Start Trial** 

Under the Data Protection Law, the employer has to take appropriate measures to ensure compliance with the principles for the processing of personal data under Article 5 of the GDPR.

Finally, special rules are provided for regarding the processing of employees' personal data through a closed-circuit recording system in the workplace, including the requirement to inform employees in a written form respectively.

### Processing of personal data for other purposes

The processing of personal data by public entities for purposes other than those for which they were initially collected is permitted if the processing is necessary for the fulfilment of their duties and if necessary:

- to check the information provided by the data subject, because there are reasonable indications that said information is incorrect;
- for the avoidance of risks to national safety, national defence, or public safety, or to ensure tax or customs income;
- for the prosecution of criminal offences;
- for the prevention of harm to another; and
- for the production of official statistics.

Processing for other purposes by private entities is permitted if necessary:

- for the avoidance of threats to national or public security following a request from a public entity;
- for the prosecution of criminal offences; and
- for the establishment, exercise, or defence of legal claims, unless data subjects' interests override.

### Processing for scientific or historical research purposes

Pursuant to Article 30 of the Data Protection Law, and notwithstanding Article 9(1) of the GDPR, the processing of special categories of data is permitted, without the data subject's consent, provided that it is necessary for scientific or historical research purposes or for purposes related to the collection or retention of statistics and data controller's interest overrides the data subject's interests. In this respect, the data controller must take appropriate and specific measures for the protection of the data subject's interests, including restrictions of access to the data controller and/or data processor, pseudonymisation, encryption, and the appointment of a DPO.

You have **4 out of 5** free articles left for the month. Sign up for a trial to access unlimited content.

**Start Trial**  


In addition, notwithstanding the provisions of Articles 15, 16, 18, and 21 of the GDPR, data subjects' rights are restricted, if their exercise could make impossible or significantly impede the performance of the scientific or historical research and so long as these restrictions are deemed necessary for their performance.

Apart from the above, special categories of data when processed for the above purposes must be anonymised, once the scientific or statistical purposes allow it, unless contrary to data subject's legitimate interest.

Finally, the data controller may publish personal data that are processed in the context of the research, so long as data subjects have consented in writing or publication is necessary for the presentation of the results of the research, in which case the publication must take place only by means of pseudonymisation.

---

## 6. PRINCIPLES

No national law variations exist.

---

## 7. CONTROLLER AND PROCESSOR OBLIGATIONS

### 7.1. Data processing notification

Following the entry into effect of the GDPR, there is no longer an obligation to notify the HDPa with regard to the processing of personal data, recordkeeping, or CCTV. In addition, the granting of licenses by the HDPa for the processing of sensitive data has been also abolished (See HDPa Decision 46/2018, only available in Greek [here](#)).

### 7.2. Data transfers

No national law variations exist.

Under Data Protection Law (see Article 28(2)(d)), certain GDPR provisions, including Chapter V of the GDPR on the transfer of personal data to third countries, do not apply to the extent necessary in order to reconcile personal protection rights with the right to freedom of expression and information,

including processing for journalistic purposes or academic, artistic, or literary expression.  
You have **4 out of 5** free articles left for the month. [Signup for a trial to access unlimited content.](#)

**Start Trial**  


In this respect, the HDPa issued recently guidance on the latest standard contractual clauses issued by the [European Commission](#) for transfers to third countries (only available in Greek [here](#)) as well as with regard to the new standard contractual clauses of the European Commission to be signed between data controllers and data processors pursuant to Article 28(7) GDPR (only available in Greek [here](#)).

### 7.3. Data processing records

No national law variations exist.

### 7.4. Data protection impact assessment

Under Article 35(4) of the GDPR, the supervisory authority establishes and makes public a list of the kind of processing operations which are subject to the requirement of a DPIA.

Pursuant to the above rule, the HDPa has issued [a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment](#). This list was adopted by means of HDPa's Decision 65/2018, (only available in Greek [here](#)).

The list includes processing activities relating to:

- systematic evaluation, scoring, prediction, prognosis, and profiling, especially of aspects concerning the data subject's economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements, or the credit rating of data subjects;
- systematic processing of personal data that aims at taking automated decisions producing legal effects concerning data subjects or similarly significantly affects data subjects and may lead to the exclusion or discrimination against individuals;
- systematic processing of personal data which may prevent the data subject from exercising their rights or using a service or a contract, especially when data collected by third parties are taken into account;
- systematic processing of personal data concerning profiling for marketing purposes when the data are combined with data collected from third parties;
- large scale systematic processing for monitoring, observing, or controlling natural persons using data collected through video surveillance systems, through networks, or by any other means over a public area, publicly accessible area, or private area accessible to an unlimited number of persons. It includes the monitoring of movements or location/geographical position on real time or not real time of identified or identifiable natural persons;

You have **4 out of 5** free articles left for the month

Signup for a trial to access unlimited content.


**Start Trial** 

- large scale systematic processing of personal data concerning health and public health for public interest purposes as is the introduction and use of electronic prescription systems and the introduction and use of electronic health records or electronic health cards;
- large scale systematic processing of personal data with the purpose of introducing, organising, providing, and monitoring the use of electronic government services;
- large scale processing of special categories of personal data referred to in Article 9(1) of the GDPR, including genetic data and biometric data for the purpose of uniquely identifying a natural person, and of personal data referred to in Article 10 of the GDPR;
- large scale systematic processing of data of high significance or of a highly personal nature;
- systematic monitoring, provided that it is fair, of the position/location of employees as well as of the content and of the metadata of employee communications with the exception of logging files for security reasons provided that the processing is limited to the absolutely necessary data and is specifically documented;
- innovative use or application of new technological or organisational solutions, which can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms;
- matching and/or combining personal data originating from multiple sources or third parties, or for two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subjects; and
- in case the processing concerns personal data that has not been obtained from the data subject and the information to be provided to data subjects pursuant to Article 14 of the GDPR proves impossible or would require a disproportionate effort or is likely to render impossible or seriously impair the objectives of the processing.

The HDPA's list is subject to regular revisions every two years or to an unscheduled revision due to significant developments in technology or in operational models, as well as in the case of a change in the purposes of the processing when these new purposes present a high risk.

Finally, according to information available on the HDPA's website, the above list is not exhaustive and, as such, the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, if the conditions of Article 35(1) of the GDPR are met, has not been removed.

The HDPA has not issued a list of the kind of processing operations for which no data protection impact assessment is required pursuant to Article 35(5) of the GDPR.

You have **4 out of 5** free articles left for the month **7.5. Data protection officer appointment** Signup for a trial to access unlimited content. **Start Trial** 

The Data Protection Law provides for specifications with regard to the appointment of a DPO by public entities, including:

- DPO's appointment (Article 6 of Data Protection Law), (e.g., one person may serve as a DPO for several public bodies, choice is made on the basis of professional qualifications, an employee of the public entity may be appointed as a DPO, provision for the notification of appointment to the HDPAs, unless not permitted for national security reasons or secrecy duties etc.);
- DPO's position (Article 7 of Data Protection Law), (e.g., participation in all matters related to data privacy; provision of necessary resources etc.); and
- DPO's duties (Article 8 of Data Protection Law), (e.g., to cooperate with the HDPAs; to act as the contact point with the HDPAs etc.).

## 7.6. Data breach notification

There are no variations with regard to the notification of a personal data breach to the HDPAs.

Data breaches can be notified electronically, (only available in Greek [here](#)). In this respect, data controllers are required to complete and submit a specific form which is available on the HDPAs' website [here](#).

Although no variations are provided with regard to notification of the data breach to the authority, the Data Protection Law provides for an exception to the obligation of data controllers to communicate a personal data breach to the data subject, in particular, when and to the extent that by means of this communication, certain information which is protected by secrecy rules would be revealed (Article 33(5) of the Data Protection Law).

Providers of publicly available electronic communications services must notify the [Hellenic Authority for Communication Security and Privacy](#) ('ADAEP') and the HDPAs in case of a personal data breach via the ADAEP's online notification form, (only available in Greek [here](#)) (Article 12(5) of the Electronic Communications Law).

## 7.7. Data retention

The Data Protection Law does not include any data retention provisions. For the data subject's right to erasure, see below under section 8.4. as regards timeframes for retaining data (although not provided in Data Protection Law), statutory (general/ specific prescription rules), or contractual retention

You have **4 out of 5** free articles left for periods would also apply. the month

Signup for a trial to access unlimited content.

**Start Trial** 

## 7.8. Children's data

Under Article 21 of the Data Protection Law, the processing of personal data belonging to a child, in relation to the offer of information society services, is lawful only if the child is at least 15 years old and provides their consent. Otherwise, children under the age of 15 must have parental or guardian's consent to be offered information society services.

## 7.9. Special categories of personal data


Notwithstanding Article 9(1) of the GDPR, the Data Protection Law stipulates that the processing of special categories of data by public and private bodies is permitted, so long as it is necessary for (Article 22(1) of the Data Protection Law):

- the exercise of rights resulting from the social security and social care right and for the performance of relevant obligations;
- the purposes of preventive medicine, the assessment of an employee's ability to work for medical diagnosis, the provision of health and social care or the management of health and social care systems and services, or by means of an agreement with a health care professional or another person also bound by professional secrecy or is under latter's supervision; or
- for the purposes of public interest in the field of public health.

In addition, processing of special categories of personal data, within the notion of Article 9(1) of the GDPR, by public entities is permitted, if (Article 22(2) of the Data Protection Law):

- absolutely necessary for reasons of public interest;
- necessary for the prevention of a significant threat for national or public safety; or
- necessary in order to take humanitarian measures, in which case the interest for the processing overrides the data subject's interest.

In all the above cases, all appropriate and special measures to safeguard data subjects' interests must be taken, taking into account the state of the art, implementation costs, the processing's context and purposes, and the severity of risk to natural persons' rights and freedoms the processing poses, including technical and organisational measures (Article 22(3) of the Data Protection Law). In addition, the Data Protection Law also allows employers, in the capacity of data controllers, to

You have 4 out of 5 free articles left for the month. Sign up for a trial to access unlimited content. [Start Trial](#) 

With regard to the processing of criminal conviction data, this is not addressed by the Data Protection Law.

### Processing of genetic data

Under Article 23 of the Data Protection Law and pursuant to Article 9(4) of the GDPR, the processing of genetic data for health and life insurance purposes is expressly prohibited.

## 7.10. Controller and processor contracts

No national law variations exist.

## 8. DATA SUBJECT RIGHTS


### 8.1. Right to be informed

When personal data is collected from the data subject, the data controller is exempt from the obligation to inform data subjects of further processing of personal data pursuant to Article 13(3) of the GDPR in the following cases (Article 31(1) of the Data Protection Law):

- the processing purpose of the further processing of personal data which the data controller stores in written form directly addressed to the data subject is compatible with the initial purpose, the communication with the data subject is not conducted via digital means and data subject's interest to be informed is not particularly high; or
- when, in case of a public body, such information would compromise:
  - the proper performance of the data controller's duties;
  - the national or public security and the data controller's interests not to provide the information override the data subject's interests;
  - the establishment, exercise, or defence of legal claims and the data controller's interests not to provide the information override the data subject's interests; or
  - the confidential transfer of personal data to public bodies.

The data controller must:

- take appropriate measures for the protection of data subjects' legitimate interests, including the provision of information outlined in Article 13(1) and (2) of the GDPR in an accurate,

You have 4 out of 5 free articles left for the month. Sign up for a trial to access unlimited content. [Start Trial](#) 



- in most cases notify the data subject in writing of their reasons for not providing the information.

In addition, broader exceptions apply for public bodies when personal data have not been obtained from the data subject, under Article 32 of the Data Protection Law.

## 8.2. Right to access

Under Article 33(1) of the Data Protection Law, the right of access is restricted when:

- there is no obligation to inform data subjects; or
- when data subjects' data:
  - was recorded only because it could not have been deleted due to regulatory provisions of obligatory retention; or
  - serve exclusively for purposes of protection or control of data,
- and the provision of information would require a disproportionate effort and the necessary technical and organisational measures to make processing impossible for other purposes.

The reasons for refusing to provide access to the data subject must be documented. Refusal to provide information should be justified to the data subject unless there is a risk to compromise purpose sought by means of refusing to provide access to the information (Article 33(2) of the Data Protection Law).

The data subject's right applies only if the data subject provides enough information to allow retrieval of data and the required effort would not be disproportionate to data subject's interest to be informed (Article 33(3) of the Data Protection Law).

The data subject's right to be informed pursuant to Article 15 of the GDPR does not apply when the information to be disclosed to the data subject should remain confidential by law or by reason of its nature, in particular, due to third parties' overriding legitimate interests.

## 8.3. Right to rectification

The Data Protection Law does not include general variations regarding the data subject's right to rectification. However, it includes limitations on the exercise of such right in the context of particular processing purposes (i.e., processing and freedom of expression and information of Article 28 of the Data Protection Law, processing for archiving purposes in the public interest under Article 29 of the

Data Protection Law and processing for scientific or historical research or for statistical purposes under Article 30 of the Data Protection Law).

You have 4 out of 5 free articles left for the month

Signup for a trial to access unlimited content.

Start Trial 

## 8.4. Right to erasure

Under Article 34 of the Data Protection Law, the right to erasure does not apply, in cases of non-automated processing, when due to the special nature of storage, erasure is impossible or is possible only following a disproportionate effort and data subject's interest for the erasure is not considered important. Also, the right to erasure does not apply when the data controller no longer needs the personal data for the collection purpose under Article 17(1)(a) of the GDPR or the personal data was unlawfully processed under Article 17(1)(d) of the GDPR, but the data controller has reason to believe that erasure would be prejudicial to the data subject's legitimate interests. In both cases, erasure is substituted by restriction of the processing. The same exception applies where erasure would be contrary to statutory or contractual retention periods. The above does not apply in case of unlawful processing.

## 8.5. Right to object/opt-out

Under Article 35 of the Data Protection Law, the right to object may not be applicable before a public entity, if the processing is required for the public interest, when the latter prevails over data subjects' interests or the processing is obligatory under a legal provision.

## 8.6. Right to data portability

There are no variations under the Data Protection Law. However, the Data Protection Law permits data controllers to restrict data subjects' right to data portability in the following cases:

- when necessary to reconcile the right to data protection with the right to freedom of expression and information, including when processing for journalistic purposes or academic, artistic, or literary expression (Article 28(2) of the Data Protection Law); and
- when the data subject's exercise of the right likely renders impossible or seriously impairs the objectives of processing for archiving purposes in the public interest and restricting the right is necessary to achieve those purposes (Article 29(4) of the Data Protection Law).

## 8.7. Right not to be subject to automated decision-making

There are no variations with regards to profiling under the Data Protection Law.

You have **4 out of 5** free articles left for  
**8.8. Other rights** the month

Signup for a trial to access unlimited  
content.

**Start Trial**  


## Right to restriction of processing

There are no variations under the Data Protection Law.

---

## 9. PENALTIES

### Administrative sanctions

In addition to the corrective powers provided under Article 58(2) of the GDPR, the Data Protection Law further specifies that public entities will be subject to the imposition of administrative fines up to €10 million by the HDPAs for the infringements included in Article 83(4), (5), and (6) of the GDPR (with a few exceptions).

The Data Protection Law introduces no variations with regard to private entities.

### Criminal sanctions

The Data Protection Law provides for the imposition of criminal sanctions and, in particular, punishment by imprisonment of up to one year, to anyone who interferes with a filing system containing personal data and by means of this act obtains knowledge thereof, copies, and generally processes personal data included therein.

Furthermore, if personal data is used, transmitted, disseminated, disclosed by transmission, made available, or communicated to unauthorised persons or the offender allows unauthorised persons to obtain knowledge of said data, the offender may be punished by imprisonment.

In case of special categories of personal data, the Data Protection Law provides for the following criminal sanctions:

- imprisonment of at least one year; and
- a fine of up to €100,000.

In addition, if the offender of the above acts had the intent to unlawfully gain an economic benefit for himself or for another person or to cause property damage to another person or harm another person and the total benefit thereof exceeds €120,000, then the offender may be punished with imprisonment of up to ten years.

You have **4 out of 5** free articles left for the month

Signup for a trial to access unlimited content.

**Start Trial** 

Finally, if from the above acts national security or the democratic functioning of the state has been put at risk, imprisonment and a fine of up to €300,000 may be imposed.

## 9.1 Enforcement decisions

### HDPA Decision 12/2021

By means of decision 12/2021, the HDPA imposed a fine of €2,000 against a company (data controller) for improper employee monitoring by means of unlawful installation and operation of a CCTV system at company's workspace in violation of Articles 5(1)(c) regarding principle of data minimisation and 6(1)(f) of the GDPR regarding the legal basis of legitimate interests. The case was investigated by the HDPA following a complaint submitted by an employee of the company alleging that the CCTV system was used for monitoring rather than for security purposes. The HDPA found that the CCTV recording was not limited to spaces that were deemed necessary for the purpose of protection of persons and goods, but rather it was also recording images from workspace which was dedicated to employees, whereas the possibility of real-time distant monitoring was also offered. The HDPA considered as aggravating factors, the fact that the data controller did not submit documentation proving the lawfulness of the entailed processing, even though requested by the HDPA. It also considered, as mitigating factors: that the company is a small company (based on the number of its employees); the CCTV system no longer operate; there is another procedure pending which does not relate to personal data; this is the first decision against the company; and the adverse economic conditions due to Covid-19 pandemic.

### HDPA Decision 13/2021

The HDPA imposed a fine amounting to €20,000 against a company with an electronic and physical store for improper response or reaction to the exercise of the right of erasure in violation of Articles 12(3) (deadline for response to a right), 17 (right of erasure), 21 (right to object), and 25(1) (protection by design) of the GDPR. The case was investigated by the HDPA following submission of a complaint based on which the complainant had received unsolicited SMS of marketing content notwithstanding the fact that the latter had previously requested erasure of his contact details (mobile number). Following HDPA's intervention, the company declared that it had erased complainant's contact information, however, it sent a new marketing SMS to him because the complainant had failed to follow the opt-out process. Instead, the latter addressed its request to the company's customer care department. Based on the HDPA this did not amount to an improper exercise of data subject's right of erasure considering that the GDPR does not set forth any such condition for the exercise of the right, Therefore, the HDPA imposed a fine for infringement of the right of erasure and for improper

You have 4 out of 5 free articles left for the month. Sign up for a trial to access unlimited content. [Start Trial](#)

process when dealing with the satisfaction of the right. The HDPa considered as aggravating factors, the fact that: the data controller did not submit documentation proving lawfulness of the erasure process; infringement related to the exercise of data subject rights; that the company had initially declared that it took all necessary measures for its entire clientele when it failed to do so; and that the company had an electronic store and should have taken actions to reply properly to data subject rights. It also considered, as mitigating factors, that: the complainant did not suffer any economic loss; that this has been the first decision against the company; and the adverse economic conditions due to Covid-19 pandemic.

You have **4 out of 5** free articles left for the month

Signup for a trial to access unlimited content.

**Start Trial**  
