Greece - National GDPR Implementation Overview

TABLE OF CONTENTS

December 2019

1. THE LAW

1.1. National implementing legislation of the GDPR

The Greek Parliament adopted, at the end of August 2019, 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 to download in Greek here) ('the Data Protection Law') which implements certain provisions of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), including with regard to child's consent, processing of special categories of personal data, processing of employees' personal data, further derogations *vis-à-vis* notice requirements, and data subjects' rights. The Data Protection Law forms currently the basic national legal framework on personal data protection in Greece along with the GDPR.

A basic feature of the Data Protection Law is the distinction made 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.

The Data Protection Law abolishes, with a few exceptions, former data protection legislation namely, Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended) ('Law 2472/1997').

Other national law provisions concerning personal data processing, as well as the Hellenic Data Protection Authority's ('HDPA') directives and regulatory acts, continue to apply to the extent that they do not conflict with the GDPR and the Data Protection Law.

The HDPA is expected to issue a recommendation in the coming months with regard to the provisions of the Data Protection Law, as well as guidance documents. In the meantime, data controllers and data processors should review their internal processes, policies, and documentation to ensure compliance with the new provisions.

1.2. Guidelines

The HDPA has released several guidelines that are addressed to controllers concerning different topics of the GDPR, such as:

topics of the GDPR, such as:

- principles relating to processing of personal data (only available in Greek here);
- guide to compliance with the GDPR (only available in Greek here);
- records of processing activities and relevant templates for both controller and processor (both only available in Greek here);
- security of processing (only available in Greek here);
- personal data breach notification;
- personal data breach notification form to be filled-in by controllers and submitted to the HDPA in an encrypted form;
- 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')
- list of the processing operations which require a DPIA pursuant to Article 35(4)
- prior consultation (only available in Greek here); and
- 'registry of Article 13' of the authority (only available in Greek here).

The HDPA also refers to the various guidelines that were issued by the European Data Protection Board, 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:

- principles relating to processing of employees' data (*see* HDPA Decision 26/2019, only available in Greek here);
- principles of accuracy and of data protection by design and by default (*see* HDPA Decision 31/2019, only available in Greek here);
- notification of a personal data breach to the HDPA (*see* HDPA Decision 14/2019, only available in Greek here);

- provision of information to data subjects under Article 12 of the GDPR (*see* HDPA Decision 15/2019, and Decision 25/2019, both only available in Greek here);
- non-compliance with the exercise of data subject's rights, namely right to access, right to erasure and right to object (*see* HDPA Decision 24/2019, Decision 27/2019, and Decision 34/2019, only available in Greek here).

The HDPA has not yet issued any decision concerning the Data Protection Law.

2. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY

2.1. 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.

2.2. 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;
- to address warnings to the controller or processor that intended processing operations are likely to infringe provisions of the Data Protection Law;
- to order the controller or 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 exercis-

ing its investigatory powers and be declared as a sequestrator until issuance of a decision by competent judicial authorities;
- to order the controller or 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; and
- to issue administrative regulatory acts in order to regulate specific, technical and detailed matters.

3. NOTIFICATION | REGISTRATION

3.1. National requirements

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 announcement and Decision 46/2018, both only available in Greek).

4. DATA SUBJECT RIGHTS

4.1. Variations of GDPR on right of information to be provided

When personal data is collected from the data subject, the 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 of the Data Protection Law):

- the processing purpose of the further processing 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 entity, such information would jeopardise:
    - the proper performance of the controller's duties;
    - the national or public security and the controller's interests not to provide the information override the data subject's interests;

the information override the data subject's interests;

- the establishment, exercise or defence of legal claims and the controller's interests not to provide the information override the data subject's interests; or
- the confidential transfer of personal data to public entities.

The 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, transparent, intelligible and easily accessible manner, in a clear and plain language.

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

4.2. Variations of GDPR on 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. In such cases, erasure is substituted by restriction of processing. The same exception applies where erasure would be contrary to conventional or legal retention periods. The above does not apply in case of unlawful processing.

4.3. Variations of GDPR on right to restriction of processing

There are no variations under the Data Protection Law.

4.4. Variations of GDPR on right to data portability

There are no variations under the Data Protection Law.

4.5. Variations of GDPR on automated individual decision-making, including profiling

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

4.6. Variations of GDPR on right to object

Under Article 35 of the Data Protection Law, the right to object may not be applicable before a public entity, if processing is required for the public interest, when the latter prevails over data sub-

jects' interests or processing is obligatory under a legal provision.

4.7. Variations of GDPR on right of access

Under Article 33 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:
    - were recorded only because they could not have been deleted due to regulatory provisions of obligatory retention; or
    - serve exclusively 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.

5. CHILDREN

5.1. National regulation of the processing of children's data and age of consent

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 its consent. Otherwise, children under the age of 15 must have parental or guardian's consent to be offered information society services.

6. PROCESSING OF SPECIAL CATEGORIES OF DATA & CRIMINAL CONVICTIONS

6.1. National regulation concerning the processing of special categories of data and criminal conviction 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 entities is permitted, so long as it is necessary for (Article 22 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 other 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 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.

7. DATA PROTECTION OFFICER

7.1. Additional/varied requirements on DPO appointment, role and tasks

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 HDPA, 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 HDPA; to act as the contact point with the HDPA etc.)

as the contact point with the HDPA etc.).

8. DATA BREACH NOTIFICATION

8.1. Variation/exemptions on breach notification obligation

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

Data breaches can be notified electronically here. In this respect, controllers are required to complete and submit a specific form which is available on the HDPA's 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 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).

8.2. Sectoral obligations

Providers of publicly available electronic communications services must notify the Hellenic Authority for Communication Security and Privacy ('ADAE') and the HDPA in case of personal data breach via the ADAE's online notification form (Article 12(5) of Law 3471/2006 transposing the Directive on Privacy and Electronic Communications (2002/58/EC) ('the ePrivacy Directive') into Greek national law (only available in Greek here).

9. DATA PROTECTION IMPACT ASSESSMENTS

9.1. National activities subject to prior consultation/authorisation

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 its 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 or through networks or by any other means over a public area, publicly accessible area or private area accessible to an unlimited number of persons. It includes the monitoring of movements or location/geographical position on real time or not real time of identified or identifiable natural persons;
- 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.

9.2. National activities not subject to prior consultation/authorisation

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.

10. PROCESSING FOR SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES

10.1. National implementation of Article 89 of the GDPR

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 controller's interest overrides the data subject's interests. In this respect, the controller must take appropriate and specific measures for the protection of the data subject's interests, including restrictions of access to the controller and/or processor, pseudonymisation, encryption, appointment of a DPO etc.

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 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.

11. SANCTIONS

11.1. 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 €10,000,000 by the HDPA 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.

A fine of €150,000 was imposed, on 30 July 2019, by the HDPA against a firm of auditors for having selected and applied an inappropriate legal basis and for having infringed the principle of accountability vis-a-vis the processing of personal data of its employees (*see* HDPA Decision 26/2019, only available in Greek here).

11.2 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 unauthorized 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.

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.

12. OTHER SPECIFIC JURISDICTIONAL ISSUES

12.1. Processing of employee data

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.

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 in particular into account:

- 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 his/her 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 and social security and social protection law, and there is no reason to consider that data subjects' legitimate interests prevail.

Under the Data Protection Law, the employer takes 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.

12.2. 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.

12.3. 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;

- 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;
- for the establishment, exercise or defence of legal claims, unless data subjects' interests override.

12.4. Accreditation of certification bodies and certification

The Data Protection Law provides that accreditation of certification bodies pursuant to Article 42 of the GDPR is made by the Hellenic Accreditation System ('ESYD') on the basis of the standard EN-ISO/IEC17065:2012 and in accordance with additional requirements set by the HDPA.

An accreditation may be revoked in cases where the ESYD is informed by the HDPA that accreditation requirements are no longer fulfilled or that the certification body is violating the GDPR and the provisions of the Data Protection Law.

12.5. Judicial protection

Under the Data Protection Law, a data subject's claims for damages against a controller or processor for violations of the provisions of the GDPR or the data subject's rights included therein, will be filed before the civil court of the registered seat of the controller or processor or before the civil court of the data subject's residence.

ABOUT THE AUTHORS

Tania Patsalia

Bernitsas Law

tpatsalia@bernitsaslaw.com

Tania is a senior associate at Bernitsas Law which she joined in 2010. Her practice is focused on EU, competition and antitrust law, advising on all aspects of antitrust, merger control and State aid rules.

Tania regularly assists clients with antitrust and competition law issues arising from their commercial arrangements and has been involved in high-profile cartel and merger control cases before the Hellenic Competition Commission. She provides clients with on-site assistance in dealing with dawn raids, including running workshops and mock exercises. Tania also advises on the application of EU law in Greece and the regulatory requirements applicable to the telecoms, media and technology sectors, regularly liaising with regulators such as the National Telecommunications and Post Commission, the National Council for Radio and Television and the Hellenic Data Protection Authority.

She provides guidance to telecoms operators on licensing requirements, compliance with their annual reporting obligations and telecoms issues relating to the use of new technologies and the launch of new products and services. Tania has broad experience in all aspects of EU and Greek data privacy rules and she routinely advises clients on the proactive identification, assessment and management of risks associated with their privacy practices. Tania assists clients in GDPR compliance steps, and advises extensively on how to identify compliance gaps and draft privacy policies, consent forms and data processing agreements. Prior to joining the firm, Tania worked as a lawyer with Ashurst LLP in Brussels as a member of their EU & Competition Law team and as a trainee at the European Commission, Directorate-General for Competition, Cartels' Unit.

RELATED CONTENT

NEWS POST

Baden-Württemberg: LfDI Baden-Württemberg publishes DSK report on GDPR implementation in English

NEWS POST

France: CNIL publishes official warning to boutique.aero

NEWS POST

Hong Kong: PCPD publishes investigation report following TransUnion data breach incident

NEWS POST

Italy: Garante announces creation of EU Coordinated Control Commission

NEWS POST

Isle of Man: Commissioner issues registration instructions for data controllers and processors