Data Protection Law Newsletter

October 2019

New Greek Data Protection Law

&

1st GDPR fine imposed by the Hellenic Data Protection Authority (HDPA)

STAVROPOULOS & PARTNERS

LAW OFFICE

NEW GREEK DATA PROTECTION LAW

&

1st GDPR FINE IMPOSED BY THE HDPA

I. NEW GREEK DATA PROTECTION LAW

Purpose

Following a fast track public consultation, the Greek Parliament adopted Law 4624/2019 (the "**Law**") with effect as from August 29, 2019 which:

- replaces the legal framework for the establishment and operation of the Hellenic Data Protection Authority (the **"HDPA"**);
- repeals law 2472/1997 on the protection of individuals with regard to the processing of personal data subject to certain provisions which remain in force;
- imposes supplementary measures in compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (the "**GDPR**"); and
- implements Directive (EU) 2016/680 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA.

Scope of application & territorial application of the Law

- The Law applies to all public and private entities/natural persons, unless process of personal data is carried out by a natural person in the course of a purely personal or household activity, whilst its territorial scope applies to all public entities and to private entities, when (only for the latter): (i) data controller or data processor processes personal data within the Greek territory; (ii) personal data are processed in the course

of the activities of the establishment of a data controller or a data processor within the Greek territory; (iii) even if the data controller or the data processor are not established within an EU Member-State or another contracting EEA member, the GDPR scope of application applies.

Specific provisions with regard to public entities

- A special legal basis is provided for the process of personal data by the public entities. Namely, public entities may process personal data when such process in necessary for the performance of a task carried out in the public interest or in the exercise of an official authority assigned to the data controller.
- The appointment, the position and the duties of the data protection officer within a public entity are specifically regulated.

Provisions supplementing GDPR

- Minors consent: Minors of at least 15 years old may grant their consent with regard to information society services.
- Processing of special categories of personal data (e.g. data revealing racial or ethnic origin, political opinions etc.) by public and private entities is permitted if it is necessary for the exercise of rights arising from the right to social security and social protection, reasons of preventative medicine, assessment of the ability of the employee to work, medical diagnosis, reasons of public interest in the sector of public health, etc.
- Processing of genetic data for health and life insurance reasons is prohibited.
- Under specific conditions expressly set out by the Law, public and private bodies may process personal data and/or special categories of personal data collected for purposes other than that for which personal data have been collected.
- Specific reference is made to the data processing with regard to the processing in the context of employment. It is expressly provided that the processing of employees' personal data is allowed only if this is deemed as necessary for the conclusion of an employment contract or the execution thereof. Where, exceptionally, such processing is legally based on the employees' consent in order for such consent to be considered as the result of free will the following are taken into consideration:
  - i) the employment contract in place; and
  - ii) the circumstances under which the consent was granted. Such consent must be granted in writing or in electronic form and it must be distinct from the employment contract. The employer must inform the employee in writing or in electronic form for the purpose of the data collection and the right of the employee to withdraw his/her consent.

    In addition, personal data may be collected through CCTV systems if such process is necessary for the protection of persons and goods. Employees

should be informed in writing about the installation and operation of a CCTV system and the data processed through such systems should not be used for the assessment of the employees' performance.

- Special provisions are stipulated in the Law with regard to the data process in the course of the freedom of expression and the right to information, for archiving purposes in the public interest and for purposes of scientific or historical research or collection and maintenance of statistical data.
- In accordance with article 23(1) of GDPR, which entitles Member States by way of a legislative measure to restrict the scope of the obligations and the rights provided for, inter alia, articles 13 (information to be provided where personal data are collected from the data subject) and 14 (information to be provided where personal data have not been obtained from the data subject) of GDPR, the Law imposes certain restrictions with regard to the right to information provided to data subjects either in the case data has been collected from such subjects or third parties.
- Right of access by the data subject, right to erasure and right to object may be restricted if the prerequisites of the Law are met. For example:
- Right of access may not be granted to data subject if data exists solely because its deletion was impossible due to legal or regulatory provisions requiring its retention, or the only purpose served is the protection and control of data whilst any provision of information would cause disproportionate effort and the required technical and operational means would make the process of data impossible for any reason other the above. In addition, such right may not be granted for reasons of national and public security or national defense.
- Right to erasure may not be granted if erasure in the course of non-automated process is not possible due to the nature of the data storage or it is possible following disproportionate effort and data's subject interest for erasure is not important.
- Right to object may not be enforced against a public entity if there is an imperative public interest for the process which prevails over the data subject's interests.

Criminal Sanctions

Except for the administrative fines set out in GDPR, the Law provides for the following criminal sanctions:

- Imprisonment of up to one (1) year to anyone who, without having the right, intervenes in a filing system of personal data and takes cognizance of such data or copies, removes, edits, harms, collects, files, organises, structures, stores, adapts, amends, restores etc. such data;
- Imprisonment to anyone who uses, transmits, disseminates, disposes, announces etc. to non-entitled persons personal data which were acquired by intervening, without having any right, in a filing system of personal data or to anyone who allows non-entitled persons to take cognizance of such data;

- Imprisonment of up to ten (10) years if an individual liable for the abovementioned acts intended to confer to himself or to another person a financial benefit or harm another person and the total benefit or damage exceeds the amount of 120.000,00€.

II. 1st GDPR FINE IMPOSED BY THE HDPA

Following a complaint, the HDPA conducted an ex officio investigation at PRICEWATERHOUSECOOPERS BUSINESS SOLUTIONS SA ("**PwC**") with regard to the process of its employees' personal data. According to the complaint, PwC informed wrongly its employees that it used consent as a lawful basis for the process of their personal data, whilst in reality the process was made under a different lawful basis of which data subjects were unaware. Moreover, following such complaint, PwC, modified its consent forms by choosing article 6b of the GDPR (i.e. process is necessary for the performance of the contract) as a new lawful basis.

The HDPA, exercising its powers conferred on it under article 58(2) of the GDPR, imposed, inter alia, a fine of 150.000,00€ to PwC for breach of articles 5 and 6 of GDPR. The main points of the HDPA's decision may be summarized as follows:

- The lawful process of personal data requires compliance with the principles set out in article 5 of GDPR. In that context, even if a lawful basis for the process of personal data exists in accordance with article 6 of GDPR, the data controller should respect the principles of lawfulness, necessity, proportionality and minimization. In other words, breach of the principles provided in article 5 of GDPR cannot be set aside because of the existence of an appropriate lawful basis;
- Selection of an appropriate lawful basis stipulated in article 6 of GDPR is closely connected to the principle of fairness and the data minimization;
- The principle of fairness establishes a relationship of trust between the data controller and the data subject;
- The data controller is obliged not only to invoke the appropriate lawful basis but to inform the data subject about such basis in accordance with articles 13 and 14 of GDRP in order to ensure transparency;
- The choice of the proper lawful basis should be made prior to the initiation of the process;
- The data processor is obliged in accordance with the principle of accountability to choose the proper lawful basis and document this choice internally in accordance with such principle;
- The HDPA underlines that the data controller under investigation is obliged, at its own initiative, to submit to the HDPA, without any questions and requests by the HDPA all measures and policies it has adopted in the context of its internal compliance. In other words, the data controller under investigation should present at its own initiative all documentation of accountability;

- The use of consent, for the process of employees' personal data is not in principle an appropriate lawful basis, due to the imbalance of power between the employer and the employee, but may be used as a legal basis only in exceptional circumstances in the context of employment relations;
- In general, consent may be used as lawful basis only where the other lawful bases do not apply. In case the data subject withdraws his/her consent it is impossible to swap to another lawful basis. Thus, refusal of consent or its withdrawal is equivalent to an absolute prohibition on the processing of personal data;
- If the data controller has doubts with regard to the choice of lawful basis, the data controller should either remove such doubts or abstain from the process of such data.

HDPA's first GDPR decision constitutes an important source for reading for all the undertakings since it analyses core principles of the GDPR model as well as clarifies the use of consent as a lawful basis for the process of personal data.

The present newsletter contains general information only and is not intended to provide specific professional advice or services.

If you need further assistance or information with regard to the above please contact:

T.Magdalinou@stplaw.com
E.Armata@stplaw.com
A.Stavropoulou@stplaw.com
