Stamatopoulos Eftychidou
legal consultans

PERSONAL DATA

UPDATED LEGAL FRAMEWORK ENTERING INTO FORCE ON 25 MAY 2018

What personal data are?

Personal data is any information relating to a natural person on the basis of which the person is identified / recognized. This may be the name, surname, VAT number, social security number ("AMKA"), and any other information that can be used to identify, directly or indirectly, the identity of a person.

In specific cases and under certain conditions, the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, restriction, erasure or destruction it is **permissible**.

All of the above actions are called processing of personal data.

What data should be protected?

Each person's personal data should be protected. That is, any information relating to an identified natural person or any information that may directly or indirectly identify an individual, in particular by reference to an identifier, such as name, identity number, location data or data relating to the physical, psychological, economic or social situation of that natural person. It is not about the data of legal persons (companies, etc.). However, it refers also to the data of a single-member company or an individual enterprise legally treated as a natural person.

The meaning of data "editing".

Editing of personal data is any act or set of operations carried out with or without the use of automated means in personal data or in sets of personal data such as collection, registration, organization, structure, storage, adaptation or alteration, recovery, search for information, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, limitation, erasure or destruction.

Therefore, processing of personal data is very broad and includes even the collection of personal data.

NEW PRIVACY FRAMEWORK

THE NEW EU REGULATION

(GDRP, ARTICLES 1-99)

The new General Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 "on the protection of individuals with regard to the processing of personal data and on the free movement of such data " **will be directly applicable on 25 May 2018** in all EU Member States, replacing the existing Directive 95/46 / EC and the national legislation that incorporated it, ie Law 2472/1997.

1. **Regulation 2016/679** "on the protection of natural persons with regard to the processing of personal data and on the free movement of such data", also known as the General Data Protection Regulation (GDPR);

2. **Directive 2016/680** "on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the enforcement of criminal penalties and the free movement of such data";

3. **Directive 2016/681** "on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offenses and serious crime".

GENERAL INFORMATION

The new General Regulation (EU) 2016/679 seeks to create a stricter institutional framework for the processing of personal data and, by extension, protection thereof.

It is characterized, in particular, by the radical change in the system of liability for compliance by introducing the Accountability Principle, according to which companies collecting and processing personal data must shape their procedures and technical and organizational systems in such a way so that they are fully in line with what the new Regulation foresees. One of the most important changes is the burden of proof. According to the new Regulation, is transferred from the Data Protection Authorities to the companies, which have to prove in any check case that they are fully in line with the provisions of the Regulation.

Furthermore, the Regulation requires a clear consent of the data subject for each processing purpose. This raises the need to immediately modernize the methods and systems used to process personal data in order to comply with strict consent and processing conditions.

BASIC ELEMENTS OF THE REGUALTION

The basic elements of the Regulation, amongst others, are:

• The need for a clear consent of the person concerned to the processing of his or her personal data (Article 7)

• Easier access of the person concerned to his / her personal data (Article 15)

• The rights of correction, deletion and the "right to be forgotten" (Article 16-18)

• The right to object, inter alia the use of personal data for 'profile formation (Article 21)

• The portability of data from a provider to another (Article 20)

Territorial scope of the Regulation:

The GDPR aims at harmonizing privacy laws across Europe, protecting EU citizens' personal data and reforming the way companies operating in the EU process personal data.

The new Regulation applies when the controller or processor

of the personal data is established in the EU, irrespective of whether the processing takes place within the Union. It shall also apply to the processing of personal data of data subjects in the Union by a controller or processors not established in the Union if the processing activities are related to:

(a) the supply of goods or services to those data subjects in the Union, regardless of whether the data subjects are required to pay, or

(b) Monitoring their behavior, to the extent that such behavior takes place within the Union. In addition, the Regulation applies to the processing of personal data by a controller who is not established in the Union, but at a place where the law of a Member State is governed by public international law.

Prerequisites for the lawful processing of personal data:

Processing is legal provided that at least one of the following conditions is met:

(a) The data subject has consented to the processing of his or her personal data for one or more specific purposes,

(b) Processing is necessary for the performance of a contract to which the data subject is a party or for action to be taken at the request of the data subject prior to the conclusion of a contract,

(c) Processing is necessary to comply with a legal obligation on the controller,

(d) Processing is necessary to safeguard the vital interest of the data subject or other natural person,

(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of public authority entrusted to the controller,

(f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, unless such interest overrides the interest or the fundamental rights and freedoms of the data subject who require the protection of personal data, in particular if the data subject is a child.

SPECIFICALLY

a. Parties involved in the processing of personal data: -

"Controller" means a natural or legal person, a public authority, a service or another body which, alone or jointly with others, defines the purposes and the manner in which personal data are processed.

- "Processor" means a natural or legal person, a public authority, a service or another entity processing personal data on behalf of the controller.

- "Addressee" means a natural or legal person, a public authority, a service or another body to which personal data are disclosed, whether a third party or not. However, public authorities likely to receive personal data in a particular investigation under Union or national law shall not be considered as recipients.

- "Third Party" means any natural or legal person, public authority, service or body, with the exception of the data subject, the controller, the processor and the persons who, under the direct supervision of the controller or executor processing, are authorized to process personal data.

b. What are the main innovations of the Regulation?

A. The new GDPR sets the obligation for the controllers to keep records of the processing activities of all the personal data for

which they are responsible, as well as the obligation for the processors to keep records of all categories of activities processing, carried out on behalf of a controller (see Article 30 of the GDPR).

A satisfactory way of preparing, both for those responsible and for the processors, is (a) to understand the issues raised by the GDPR (awareness), (b) to record the data (inventory) and procedures, systems and records (physical and digital) containing them (data mapping); (c) the analysis of the deviation from compliance with the GDPR (GAP analysis) (d) designing (or redesigning) appropriate policy flows and processes carried out so that the player is able to watch and set up a record keeping system.

B. Introduces the Data Protection Impact Assessment (DPIA) responsibility for data protection in specific processing categories. In particular, the controller is explicitly obliged to conduct a DPIA prior to critical processing whenever a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of such processing, may result in a high risk to the rights and freedoms of data subjects. (See Article 35 (1) GDPR.

C. An obligation for categories of controllers and processors to establish a Data Protection Officer (DPO) on the basis of specific quality criteria, including the execution of specific types of processing. It also defines the cases of obligatory DPO designation and allows the controller or processor or associations and other bodies representing categories of persons responsible or processors to designate a DPO and, in addition to the mandatory definition thereof.

The existence and operation of the DPO is extremely important for companies because it will essentially be the person who will direct the organization towards completing and adhering to a good compliance program with the GDPR, will handle any complaints and infringements and will represent the company in the supervisory authority on all relevant issues. For this reason, even when the appointment of a DPO is not mandatory, it would be particularly beneficial for each company to voluntarily appoint a DPO. The GDPR does not provide for specific criteria or certifications for the selection of the DPO, but considers that it should be a person with extensive experience in the legislation on personal data and the management of any relevant breaches.

D. The new GDPR encourages in particular, the drafting of codes of conduct by associations and other bodies representing categories of controllers or processors in order to determine the application of the GDPR (Article 40 of the GDPR) and the establishment of data protection certification mechanisms to demonstrate compliance to the GDPR (Article 42). It is noted, of course, that both of these cases do not act as an excuse for liability.

Administrative fines.

To ensure compliance with the new rules the new Regulation introduces administrative fines in the event of a violation of the provisions of the Regulation, unless other measures are taken.

Thus, specific breaches of the obligations of those responsible and processors incur fines of up to € 10,000,000 or, in the case of enterprises, up to 2% of the total annual turnover of the previous financial year (whichever is higher). It is also a characteristic fact that this lack of appropriate organizational measures to comply with the GDPR may also result in the fine being imposed, without even being infringed. Heavier fines are reserved for

violations of data subjects' rights, basic principles for processing, the transfer of personal data to a recipient in a third country or an international organization, and non-compliance with a mandate or temporary or definitive restriction processing or suspending the data traffic imposed by the supervisory authority or not providing access.

In such cases, administrative fines of up to € 20,000,000 or, in the case of businesses, up to 4% of the total annual turnover of the previous financial year, whichever is the higher, are imposed.

IN CONCLUSION

The new Regulation seeks to ensure a balance between the continuous flow, collection and processing of personal data and the inalienable rights of protection that must be preserved and updated.

The subject of the personal data may now bring to court both the controller and the processor.

They therefore jointly and severally liable (the person responsible and the processor), which liability did not exist to date, as liability was exclusively acknowledged on the controller.

The regulation of the processing and protection of personal data is equivalent to rebalancing the economic activity of the business, but also of our daily routine for the protection of the personal data preservation.

In this respect, the new Regulation is a new and necessary step forward, both in terms of enhancing the law of personal data protection and in fostering a self-regulatory culture of businesses and actors to protect the personality of the individual.

Stamatopoulos Eftychidou
legal consultans

www.stameft.com
11, Mavrokordatou str. Athens, 106 78
E. info@gstamlaw.com; info@stameft.com
T. 0030 2103808701