EROTOCRITOU

ADVOCATES - LEGAL CONSULTANTS

The new Data Protection Regulation: How does it affect you?

August 22, 2017

After years of preparation and debate, the European Union Regulation on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data ("General Data Protection Regulation" or "GDPR") was finally approved by the European Parliament in April 2016.

In an effort to simply and streamline data protection across the region, the GDPR establishes a uniform set of rules to be applied consistently in all member states.

The GDPR replaces the currently applicable Data Protection Directive 95/46/EC and will take effect after a two-year transition period. Until now, the transposable directive meant that companies were subject to differing rules and processes depending on the implementation measures taken by the member state with which they were dealing.

What is personal data?

Personal data is information voluntarily transmitted by individuals (for instance: as part of a form) or collected as a result of their activity (for instance: purchasing history). The definition given in the Regulation states that personal data is any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

What benefits does the new Regulation create for individuals?

In an effort to strengthen citizens' fundamental right to the protection of personal data, and build trust in companies that collect such data, the GDPR provides individuals with the following tools for gaining control of one's personal data:

(a) The largely publicized "right to be forgotten" gives an individual, who no longer wants her/his data to be processed, and provided he/she shows that there are no legitimate grounds for retaining the data public, the right to have the data deleted.

(b) The GDPR aims to give individuals easier access to their own data through rights such as the right to have access to information on how their data is processed but also a portability right facilitating the transfer of personal data between service providers.

(c) Data protection by design' and 'Data protection by default' are now essential elements in the EU data protection framework. Data protection safeguards will be built into products and services from the earliest stage of development, and privacy-friendly default settings will be the norm – for example on social networks or mobile apps.

What benefits does the new Regulation create for companies?

(a) The GDPR was designed to harmonize data privacy laws across the EU by creating a single, pan-European law for data protection, replacing the current inconsistent patchwork of national laws. Companies will deal with one law, not 28.

(b) The GDPR provides for the creation of the European Data Protection Board (EDPB). This "one-stop-shop" for businesses whereby they will be answerable and will have to deal only with a single supervisory data protection authority and not individual national authorities.

(c) The current framework places EU companies in a position where they have to adhere to stricter standards than companies established outside the EU but also doing business in the Single Market. The GDPR establishes a principle whereby the same rules apply for all companies, regardless of where they are established. If the organisation offers goods or services to, or monitors, processes or holds data pertaining to data subjects residing in the EU, then the Regulation applies regardless of where the company itself is located. Accordingly, companies based outside of Europe will have to apply the same rules when they offer goods or services in the EU market.

All of these measures will cut costs significantly for businesses whilst also levelling the playing field between small and large players but also between EU and non-EU players. Most importantly however, a single set of rules will have a significant impact on businesses and enhance the attractiveness of Europe as a location to do business while at the same time strengthening the EU in its global promotion of high data protection standards.

What obligations does the new Regulation impose on companies?

The GDPR places certain obligations on companies that collect or process personal data or that determine the purposes and means of the processing of personal data. Such companies are labelled as "data controllers".

The GDPR contains an obligation that personal data should be processed in a manner that ensures appropriate security of personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing. Therefore, the controller or processor should evaluate the risks inherent in the processing of personal data and implement measures to mitigate those risks. (Art. 32 of the GDPR). Where processing is based on consent, the controller must be

able to demonstrate that the data subject has actually and effectively consented to processing of his or her personal data.

Alongside the right of individuals to access their personal data, the GDPR creates an obligation on companies to notify without undue delay, and no later than 72 hours, the national supervisory authority (in Cyprus the Data Protection Commissioner) and the individuals themselves, of data breaches which put individuals at risk and communicate to the data subject all high-risk breaches. Such a notification duty is only exempt if the controller is able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

What are the penalties for non-compliance?

The GDPR contains clear rules on conditions for imposing administrative fines. Data protection authorities will be able to fine companies who do not comply with EU rules, if they have for instance not informed their clients that they're data have been breached or the data protection authorities.

As of the 25th of May 2018, organizations in non-compliance can be fined up to 4% of annual global turnover for breaching GDPR or €20 Million. This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

“Stronger rules on data protection from May 2018 mean citizens have more control over their data and business benefits from a level playing field. One set of rules for all companies operating in the EU, wherever they are based.”

When does the GDPR become effective?

Unlike the Directive, and given the nature of a Regulation, the GDPR does not require any enabling national legislation to be passed, meaning it will be directly applicable in all member states as of May 25th 2018.

In the meantime, in Cyprus, the national framework (‘The Processing of Personal Data (Protection of the Individual) Law of 2001’ 138 (I) 2001) remains applicable. The 2001 law entered into force in order to address privacy issues related to the collection, storage, processing, dissemination and use of such data. It was amended in 2003 in an effort to implement the 95/46 Directive. By May 2018, the GDPR will replace this framework and will be both applicable and enforceable to companies established or operating in Cyprus.

The changes will give people more control over their personal data and make it easier to access it. They are designed to make sure that people's personal information is protected – no matter where it is sent, processed or stored – even outside the EU, as may often be the case on the internet.

The Data Protection Commissioner in Cyprus has been traditionally reluctant to impose fines for breaches of the 2001 law and preferred issuing warning letters instead. The new GDPR rules may bring about changes in the Commissioners tolerance policy as a stricter approach is to be implemented. It remains to be seen whether fines start becoming common place.