RCD ALERT

December 2017

PRIVACY AND DATA PROTECTION

COUNTDOWN FOR THE APPLICATION OF THE EU GENERAL DATA PROTECTION REGULATION

ABSTRACT

The General Data Protection Regulation (GDPR) shall apply from 25 May 2018. The GDPR expands the obligations and responsibility of the companies and entities when processing persona data, and the privacy rights of the citizens as well. The GDPR also applies to entities not established in the Union when they process personal data of citizens who are in the Union. It foresees important fines for infringements of the basic principles for personal data processing, and underlines the obligations of prevention and accountability. The GDPR must not be seen as a threat, but as an opportunity, though companies and entities must seek proper assessment in order to put in place the necessary measures, within their respective organizations, to comply and to be able to demonstrate compliance with the GDPR by 25 May 2018.

The General Data Protection Regulation (GDPR), Regulation EU 679/216, of 27 april 2016, shall apply from 25 May 2018, date from which it shall be binding in its entirety and directly applicable in all Member States.

The GDPR shall apply to any company or entity established in the EU, and to those not established in the EU if they process personal data of citizens who are in the Union, either for offering goods or services, or monitoring their behavior within the Union (art. 3 GDPR), in which cases they shall designate in writing a representative in the Union to be addressed by authorities and data subjects (art. 27 GDPR).

The GDPR is based upon prevention and the principle of 'accountability' of companies and entities, so that every organization shall be responsible for, and be able to demonstrate compliance with the GDPR (arts. 5.2 y 24.1 GDPR).

It is therefore necessary that companies and entities seek proper assessment and evaluate their current data processing policies, in order to determine the appropriate measures, consistent with their business models, and taking into account the costs of implementation and the risks for the data subjects, in order to make sure they will comply with GDPR.

The GDPR grants new rights for data subjects, additional to those already known rights of access, rectification, erasure or blocking, or the right to object, like for instance the expanded right to erasure or 'right to be forgotten' (art. 17 GDPR), the right to restriction of processing (art. 18 GDPR), the right to data portability including the right to having the data transmitted directly between companies (art. 20 GDPR) or the right not to be subject to decisions based solely on automated processing, like profiling (art. 22 GDPR).

The aforementioned extension of the rights of the data subjects entails, in turn, a wide range of complementary obligations for companies and other operators such as:

- the data protection by design (for example, when a new mobile application is being developed) and by default, in order to ensure that personal data are not made accessible without the individual's intervention to an indefinite number of natural persons (art. 25 GDPR);

- to maintain (organizations employing more than 250 persons or processing sensitive data, like data concerning health, sex life, etc.) a record of data processing activities (art. 30 GDPR), which by the way will replace in Spain the traditional obligation to register the personal data files with the Data Protection Agency;
- to notify and to communicate to the authorities and to the data subjects in case of personal data breaches (hacking, virus, etc.) resulting in risks (arts. 33 y 34 GDPR);

- to evaluate appropriate security measures consistent with risks, like encryption and pseudonymisation (art. 32.1 GDPR) and to implement them;

- in certain cases, to designate a Data Protection Officer to monitor compliance with the GDPR and to act as contact point for the supervisory authority (arts. 37-39 GDPR); or

- also in certain cases, to carry out an assessment of the risk on the protection of personal data prior to the processing, in particular when using new technologies (art. 35 GDPR).

On the other hand, it is advisable, as a hallmark in the management of data protection, that companies and entities consider adherence to codes of conduct (Article 40 GDPR) in which the specific practices of a sector are detailed, including regarding data protection, for example in relation to issues such as pseudonymization or information provided to children and their protection, since this can be taken into account positively in the evaluation of possible fines.

And we cannot fail to make a reference, precisely, to the system of fines (Article 83 GDPR) foreseen by the GDPR, which basically establishes two lists of obligations whose infringement would be subject to administrative fines up to 10 or 20 million euros, or up to 2% or 4% of the total worldwide annual turnover of a company (whichever is higher), respectively, the infringement of the basic principles for processing the data subject's rights being among the causes of application of the highest fines.

In short, the GDPR aims to create a European space of trust that precisely promotes the development of the economy in the digital era, dominated by online activity and cross-border flows of personal data, every second, on an unprecedented scale until now, and in all sectors of activity.

For that reason, the GDPR should not be considered by companies as a threat, or a bureaucratic and limiting burden of doing business (as indicated by the GDPR (Recital # 4), "the right to the protection of personal data is not an absolute right "), but as an argument for positioning and as a business opportunity, totally compatible with the necessary and legitimate development of the economy.

The priority given by each organization to this question and the transparency with which it manages the privacy issues will undoubtedly be a competitive and differentiating factors of each entity, which explains why the GDPR itself obliges the Member States to encourage the establishment of data protection certification mechanisms, seals and marks allowing entities to demonstrate to their stakeholders compliance with the GDPR (Article 42.1 GDPR).

DO YOU HAVE ANY QUESTIONS?

We in the Privacy and Data Protection Department work to clarify any doubts or questions regarding the new regulation and how it could affect the activity of various businesses and organizations. If you have any questions, please do not hesitate to contact us.

CONTACT:

Privacy and Data Protection Department at RCD

rcd@rcd.legal

+34 93 503 48 68

+34 91 758 39 06