AUGUSTA
ABOGADOS

INFORMATIVE COMMERCIAL FLASH AUGUSTA ABOGADOS

ENTRANCE IN APPLICATION OF THE NEW EUROPEAN REGULATION OF DATA PROTECTION: ARE WE REALLY PREPARED?

For a long time, it has been announced and now we are at the doors, after the two years provided for the companies and the public bodies to adapt to the new regulation: **from May 25, 2018** the Regulation (EU) 2016/679 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 and on the free movement of such data ("**DGPR**" or "**Regulation**") will be applicable.

This Regulation supposes a clear change of paradigm: this Friday the regulation regarding data protection has been harmonized all through Europe. From now on, the system will start to be based on active responsibility, a system that transfers the responsibility to the data controllers or processors to determine which are the appropriate measures to guarantee, before any data processing, the rights that the Regulation grants to the holders of those data rights. The change is substantial, as it implies the entire population awareness of the fact that personal data are property of each owner ant that, therefore, this data shall not be collected without informing and obtaining the owner's consent to carry out all the actions concerning their data, empowering owners to exercise their rights in the event of any violation.

As a reminder…

Data protection is a concept created to safeguard the data which can lead to the identification of a physical person. These data include: name, surnames, e-mails, personal domicile, date and place of by birth, ID card, voice and image, handwritten and electronic signature, sanitary card, print and other biometric data, telephone number, IP directions, license plates, physical traits, among other things.

In Spain this concept is set as a fundamental right which grants citizens the control of their personal data and the capacity to make their own decisions about its disposal. The Spanish Constitution reflects this right in its article 10, relative to the dignity of the individuals, and in its article 18.4, in which it is stated that the Law will restraint the use of the computer to guarantee the honour and the personal and familiar privacy of the citizens as well as the full exercise of their rights.

The RGPD constitutes the beginning of an integral modification of the data protection regulation: the entrance into force of the regulation implies the derogation of Directive 95/46/CE, which until now stablished the inspirational frame so each Member State of the European Union could determine its own data protection rules. In Spain, the transposition resulted in Organic Law 15/1999, of December 13th, of Personal Data Protection ("**LOPD**") together with its development regulation, the Royal Decree 1720/2007, of December 21st, which approves the regulation for the development of the LOPD. Notwithstanding the above, the DGPR does not imply the automatic derogation of national rules, which will simply apply as default. The DGPR is a European regulation and, hence, directly applicable within all Member States, which means national judges must apply it before national rules.

The next step towards completing the adaptation corresponds to the Member States' Parliaments, which must modify their rules to avoid any possible conflict with the DGPR forecasts. With this purpose, the Spanish Parliament is currently developing an Organic Law for the Personal Data Protection ("**Project**"), regulation by means of which the LOPD and its complementary norm will be derogated and will imply a new frame for the measures of data protection in compliance with what the RGPD establishes.

It seems that, for the moment, the Data Protection Spanish Agency ("**AEPD**") will continue to be a baseline monitory body for the fulfilment of the new rule in Spain, being also an attendant for the tasks of population awareness. In this regard, the AEPD has been publishing via its website a series of guides and tools to facilitate employers and freelancers the identification of the measures which need to be adopted, all with the aim of achieving an application and fulfilment of the new regulation.

Hereunder, we describe the most significant changes:

- The change in the **system of active responsibility** regarding the controllers or processors of the treatment, and therefore turning the addressees of the Regulation into contributors of its application. As it has been mentioned before, the latter implies a previous treatment analysis and the subsequent adoption of measures which are considered suitable to guarantee the fulfilment of all the requirements disposed by the regulation frame, making the company liable for even the selection of third suppliers. This exercise of analysis will have to be carried out from the data owners' prospect of interest and not from the company's prospect of interest.

- The obligation to **collect the specific consent, informed and unambiguous** for the treatment of any personal data, indicating previously at least: the purposes of the treatment, the addressees of the information (identification of the controllers or processors in case of cession or international transfers of data), the term or the criteria for the conservation of the data, when appropriate, the indication of the existence of automated decisions or profile preparations and the eventual existence of a Data Protection Officer, the compulsory or facultative nature of the answers to the questions raised and their implications, the possibility of using the rights established in the Regulation and the right to present a claim in front of the AEPD.

- As for the rights commonly known as ARCO, which are the right to **access**, **rectification**, cancellation (from now on also known as the right **to forget**) and **opposition**, the new regulation adds the following: a right of **limitation**, with regard to the impossibility of using the data for purposes for which the owner has not been informed; and the right of data **portability**, which refers to the owner's right to obtain a copy of the data that he has facilitated.

- Both Public Administrations and private sector companies that carry out treatments that require a usual or systematic observation of individuals, and hence treat special data (ideology, union membership, religion, beliefs, racial origin, health or sexual life) will have to appoint a **Data Protection Officer** (known as DPO). This figure may be represented by an internal or external person of the company, provided that this commissioned has juridical and practical knowledges regarding data protection and has no conflict of interest with the exercise of this position.

- Those companies that employ more than 250 employees or, in spite of employing a lesser number, carry out a data treatment which may imply a risk for the rights and freedoms of the interested or may include special categories of data, shall be forced to keep a treatment activities register indicating the following: the origin of the data, the categories of the data (employees, customers, suppliers, images…), the files or supports in which it is contained, the identification of the data communications, its time of conservation and its process.

- There is a **new monetary sanction regime**, which classifies them in two different typologies depending on their severity: the less serious acts will be sanctioned either with an amount of up to 10M Euros or a 2% of the company's annual turnover (applying the highest of both numbers), whereas the most serious acts will be sanctioned with either fines of up to 20M Euros or a 4% of the company's annual turnover (also applying the highest number).

  The DGPR foresees the possibility of, in some cases, substituting the economic sanction by the **prevention**: this will involve the forcing of the company to adopt the preventive measures indicated by the organism of reference of each country.

  Likewise, it is necessary to consider that the DGPR also foresees the possibility of the affected lodging a claim for the damages suffered by the data disclosure.

We can conclude that the big changes introduced by the regulation since today are (i) the change in the liability, limited until now due to the fulfilment of what was stated in the LOPD; (ii) the non-obligation to register the data protection files in the AEPD; (iii) the impossibility to collect the consent for the data treatment tacitly and (iv) the fact that having a security document is not compulsory anymore, although it is still recommended its possession and update.

As we have mentioned previously, the changes established by the Regulation constitute only the beginning of the regulation change, which will conclude with the coming into force of the new Project. For now, all we have are the application guidelines, but it will be necessary to see the final scope of each of the obligations.

Author: Ana Martínez Bonet