SQUIRE PATTON BOGGS

Spanish Corporate-Real Estate Legal Update nº 32. December 2016

Main New Aspects Introduced By the Recent European Data Protection Regulation

After a legislative process spanning more than four years, in April 2016 the European Parliament approved the new Data Protection legal package through Regulation 2016/679, of 27 April, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "Regulation").

The Regulation fulfils the main goal: to renew and replace the regulatory framework throughout the EU, for application to all member states with no need for transposition into national regulations.

Although many of the principles and obligations established in the Regulation are already applicable under rules already in place, the Regulation introduces several new aspects, most notably:

- The **territorial scope of application** – The Regulation applies to data controllers or processors (i.e. the entities, persons or administrative body deciding on the purpose, content and use of personal data processing) established in the European Union, but it broadens the territorial scope of application to include controllers and processors that are not established in the EU, provided the processing is a result of an offering of goods or services aimed at EU citizens, or as a result of a monitoring and tracking of their behaviour (e.g. tracking via cookies).
- In general, the requirements and conditions for **obtaining consent** from data subjects are rendered more stringent. It is now necessary to obtain "a statement or clear affirmative action", instead of tacit consent as has hitherto been the case. Specific conditions are also established for obtaining the consent of minors.
- The information which must be provided on **data processing** is now broader than the information envisaged in current Spanish legislation (Organic Law 15/1999, of 13 December, concerning Personal Data Protection (LOPD)). For example, the Regulation requires that the identity and contact information of the controller and their representative be provided; that the purpose and the legal grounds for processing the data be provided; and that the persons or categories of persons to whom the data will be provided, where applicable, should also be stipulated. This information may be provided in combination with standardised icons for all EU countries.
- An **"accountability system"** is established for the controller, which means the latter must establish appropriate technical and organisational measures to guarantee and prove that the data processing is conducted in accordance with the Regulation.
- Likewise, the controller must conduct Privacy Impact Assessments (PIAs) for data processing operations whenever these are likely to pose a high risk for the rights and freedoms of the data subjects. For this purpose, in certain cases said assessments are mandatory, such as the large-scale processing of special data categories or personal data concerning criminal convictions and offences based on automatic processing, such as profiling, and on the basis of which decisions with legal effects for the personas are made. Should the impact assessment reveal that the processing would pose a high risk, the controller must previously consult the supervisory authority.
- The rights of the data subjects are also reinforced, with the **right to be forgotten** as part of the right to erasure, and including: (a) the **right to limit processing**, which is the right to the controller's restricting the use made of the data, (b) **the right of data portability**, i.e., the data subject's right to receive from the controller the data concerning him in a structured, commonly use, mechanical format, and (c) **the right to oppose decisions based solely on automatic processing**, including the compiling of profiles with legal or other significant effects on the data subject.
- The responsible party must keep a **record of processing activities** which will be available to the supervisory authority, although this obligation does not apply to companies with fewer than 250 employees, unless the processing might pose a risk to the rights and freedoms of the data subjects, is not occasional, or includes special categories of personal data or personal data concerning criminal convictions and offences. In contrast to the present regulatory framework, which requires that organisations register their files with the Spanish Data Protection Agency, the Regulation focuses on internal registration obligations. The information to be stored is similar to the information currently registered with the Spanish Data Protection Agency through the declaration of files via the official form (the NOTA form).
- The controller must **notify** the supervisory authority **of any breaches of security** without undue delay and in a maximum of 72 hours, unless the risk to the rights and freedoms of the data subjects are low. There is also an obligation to notify the data subjects in regard to such breaches when they pose a high risk, with a few exceptions.
- In line with the current trend of having specific persons performing specific duties in companies to ensure regulatory compliance (compliance officers), the Regulation introduces the mandatory figure of the **Data Protection Officer** (DPO) in certain spheres. The DPO must be a person with specialist knowledge of the matter, employed by the company or not, who will participate in, supervise and advise on all aspects relating to data protection, acting as a conduit for the supervisory authorities and the data subjects.

- The Regulation introduces the "one-stop-shop" principle which, in certain circumstances, allows the supervisory authority in the location of the main premises of a controller, to act as the main supervisory authority in cross-border data processing and to undertake procedure coordination tasks related to infringements.
- The **penalties** have been increased considerably. In particular, the Regulation envisages fines of up to €20 million or 4% of total annual overall turnover in the previous tax year, whichever is higher.
- Similarly, the Regulation promotes the preparation of **codes of conduct** to support the application of and compliance with the rules, and the creation of certification mechanisms to prove compliance with data protection obligations.
- Genetic and biometric data have been added to the list of **data considered to be especially protected**.
- The restrictions are maintained on the **transfer of data to third countries** in respect of which there is no decision on sufficiency by the Commission, although it is envisaged that, when the transfer is conducted using sufficient guarantees (such as the standard clauses adopted by the Commission or binding corporate standards), no authorisation will be required from the supervisory authorities.
- Establishment of **compliance seals** (European Seal).

Consequently, we can conclude by saying that the changes most likely to affect organisations are: the internal record all companies must keep of the activities involving any kind of data processing; the appointment of a DPO; the concept of consent through a clear affirmative action; the pro-active responsibility of companies to prove that they have fulfilled these obligations (through internal policies, procedures, controls, etc.); and the impact assessments that companies must conduct to analyse any potential risks arising from data processing.

Lastly, the mandatory deadline for companies to adapt their internal rules to the provisions of the Regulation is 25 May 2018. Although this deadline may seem ample, given the importance of the actions to be implemented and the scale of the penalties for non-compliance, we advise that companies start adapting their internal rules to avoid any potential non-compliance.