New data protection rules: main highlights

Isabela Crespo Vitorique
Senior Associate of the IP-IT Practice Area, Gómez-Acebo & Pombo

At long last, following its adoption last 14 April 2016, the official text of the new General Data Protection Regulation - Regulation (EU) 2016/679 of the European Parliament and of 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 - was published in the Official Journal of the European Union on 5 May 2016. As of that date, the time limits specified in the text itself started running: twenty days following the date of publication for its entry into force, thus coming into effect on 24 May 2016, and the two-year transitory period for its application elapsing on 25 May 2018.

The new European regulation is composed of a total of 173 recitals and 99 articles divided into 11 chapters, repeals Directive 95/46 and seeks to, on the one hand, strengthen the rights of data subjects and, on the other, improve opportunities for organisations in the context of the digital single market.

After a lengthy passage and the numerous alterations the legislative text has undergone throughout the same, attention is here drawn, in the form of highlights, to the main issues or developments that organisations acting as data controllers or data processors should pay heed to:

1. Territorial scope

The Regulation applies, on the one hand, to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not, and, on the other, the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

The Regulation also applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

2. Information and consent

Controllers should review, in order to ensure compliance with the provisions of this new piece of legislation, their information and transparency procedures in respect of users so as to strengthen them even further, if possible, inasmuch as the information provided must be clear, transparent and easily accessible. Processors will have to assume new direct obligations concerning security measures and, where appropriate, the notification of breaches.

3. New rights: rights to erasure (right to be forgotten), to data portability and to restriction of processing

Organisations will have to adapt their internal procedures to the new rights recognised by the Regulation, namely, the right to erasure (right to be forgotten) or right to erase data when not relevant, the right to data portability or right to receive data provided to a controller and to transmit such data to another controller and the right to restriction of data processing where one of a set of circumstances apply, including, for instance, the controller no longer needing the personal data for the purposes of the processing, but being required

by the data subject for the establishment, exercise or defence of legal claims.

4. New principles: accountability, data protection by design and data protection by default

There are three new principles to which the Regulation applies: accountability or responsibility for and ability to demonstrate compliance with the principles relating to processing of personal data; privacy by design or implementation of appropriate technical and organisational measures in order to meet the legislative requirements and protect the rights of data subjects; and, privacy by default or ensuring by default that only personal data which are necessary for each specific purpose of the processing are processed.

5. Records of processing activities

Among the new developments found in the Regulation is the creation of records of processing activities, which means that each controller and, where applicable, the controller's representative or processor, must maintain a record of processing activities under its responsibility. Such record shall contain information determined by the Regulation itself.

6. Notifications of personal data breaches to the supervisory authority

In the case of a personal data breach, the controller shall without undue delay and not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

7. Impact assessments

Data protection impact assessments are treated here as an exercise in risk analysis of a particular information system, product or service in order to address the effective management of identified risks through the adoption of appropriate measures. The Regulation provides for the same where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.

8. Data protection officer

The designation of a data protection officer is optional, except in those cases where:

a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

9. International data transfers

Given the recent changes in this area, data transfers should be reviewed, especially those made to the United States of America on the basis of the new "Privacy Shield" agreement

10. Penalties

Organisations will undoubtedly have to bear in mind the new penalty regime which, depending on the infringement, may entail fines up to 20,000,000 EUR or an amount equivalent to up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

To conclude, a review and adaptation of systems and policies has been ushered in for organisations that act as controllers or processors in order to ensure compliance with the provisions of the new General Data Protection Regulation.