BBVA Research

European regulatory process on privacy and personal data protection

Carmen Cuesta / David Tuesta
04 Jun 2014

- This paper contains an analysis of the main changes introduced in the European Parliament's legislative resolution, dated 12 March 2014, on the proposed European Parliament and Council regulation to protect individuals' personal data and on the free movement of such data (General Data Protection Regulation).

- The regulation's original text, proposed by the Commission on 25 January 2012, was very controversial, with much pressure being exerted from many sectors, corporations and even regulators outside Europe, who view a strict European law on privacy as representing a hindrance to much of the international business being conducted by their companies.

- The European Parliament's position has required a re-writing of nearly every clause of the original text, trying to balance positions which maintain that a laxer use of data encourages greater economic growth, with others prioritising consumer rights protection.

- The most important changes relate to (i) creating profiles, (ii) defining pseudonymous data, (iii) making it mandatory to include data protection premises when designing processes, (iv) developing a "European Stamp for Data Protection", and (v) toughening sanctions.

- The law does not make major changes to international data transfer, an area which is still in need of close international collaboration.

Background

Privacy is protected under article 12 of the Universal Declaration of Human Rights (1948), under article 17 of the International Pact of Civil and Political Rights (1966), as well as in many other international and regional Human Rights treaties. Practically all countries in the world include the right to privacy in their constitutions, regulating the relationship between the state, public and private institutions and citizens with regard to privacy and personal data protection.

Europe is the region with the most developed regulation on privacy. “Directive 95/46/EC relative to the protection of individuals in the treatment of personal data and the free circulation of data” was passed in 1995 with the purpose of harmonising member states’ legislation and of setting out shared principles which would encourage the creation of the European Single Market. However, ***the national transpositions by Member States have resulted in the coexistence of different regulations, resulting from different interpretations.***

Conscious of the existing fragmentation between member states and of the social change caused by the mass adoption of new technologies and new ways of sharing personal information, the European Commission proposed legislative reform at the beginning of 2012. This consisted of (i) regulation to be applied directly in all member states setting out a general framework for personal data protection in Europe, and (ii) a new Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

After more than 3,000 amendments and a plethora of proposals from consumer associations, business sectors and several industry segments, on 12 March 2014 the European Parliament finally agreed its position on the Commission’s proposal. The ordinary legislative procedure is being followed, so the Council’s opinion has yet to be formulated, and consensus positions then found between the Commission, Parliament and the Council (trilogues). Even so, the **approval of the text by the Parliament before the European elections represents a step forward in the legislative process**, which will probably not be complete until well into 2015.

The sections below cover the key new content incorporated into the regulation by the Parliament.

Profiling and pseudonymous data

Progress in information technologies has sparked a revolution in the way in which society has been moving into the digital era in the last few years. The proliferation of mobile devices and the global roll-out of telecoms networks have brought mass access to digital services for information, leisure, health, education, etc. Social media, for example, enable people on opposite sides of the world to connect with one another and provide a forum for sharing knowledge, information, resources, etc. Access to e-mail accounts or downloading resources such as documents, applications or files are examples of services that are provided free to end users. In exchange, the institutions providing these services receive personal information with which they can build value, or ”sell” to other companies the option to exploit the collected data so as to improve their knowledge of potential customers’ tastes, preferences and consumption patterns. **Profiles generated based on preferences, tracking, digital footprints, internet browsing patterns, social media, etc. thus become a good with economic value.**

When data are collected without the permission of the data subject, wherever the data comes from, even from public records, individual rights may be compromised, since the individual may feel subjected to tracking and surveillance breaching his privacy.

Parliament, with consumer rights in mind, stresses that the measures that have been introduced by the Commission are designed to regulate profiling, starting from the assumption that every individual should be able to prevent profiling using data about them (article 20). The modification of paragraph 5 of article 20 is particularly important. This requires “the right to obtain human assessment and an explanation of the decision reached after such assessment … in the case of profiling which leads to measures producing legal effects concerning the

data subject or does similarly affect [their] interests, rights or freedoms". ***The aim is to restrict the results that can be obtained using automated Big Data operating techniques.***

But on many occasions, profiling using the data provided does not involve processing data on the people about whom the information is collected, but is rather behaviour modelling. ***In these cases, the data subject suffers no intrusion into their privacy***, while the institution exploiting the data can generate value using the profile created, providing a service, for example, to other individuals who have consented to having their data contrasted with defined patterns. The definition of pseudonymous data ("personal data which cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution") introduced by the Parliament is good news for those defending the economic contribution which profiling can make to society. The clarification of recital 58a (new), which makes clear that profiling based solely on the processing of pseudonymous data does not significantly affect the interests, rights or liberties of the party involved, means that this activity involves no specific risk in personal data processing and as such is exempt from actions defined in the new article 32a. These actions include, for example, the designation of a data protection officer and the need to carry out a data analysis impact assessment. Here it is important to mention the changes introduced by the Parliament in the need to apply protection measures commensurate with the inherent risk of processing, outlined in article 32a, given that they specify in more detail those operations which present specific risks.

Introducing the concept of pseudonymous data may give breathing space for handling personal information and thus obtaining value from personal data which will undoubtedly encourage innovation and economic development.

When it comes to completely anonymous data, recital 23 establishes that this is beyond the scope of the regulation, provided the information concerned does not refer to an identified or identifiable individual. In any event, the European Data Protection Supervisor is charged with publishing directives and recommendations specifying which criteria and conditions are applicable to profiling.

"Privacy by design" or the inclusion of privacy requirements when designing products and services

Several clauses of the text refer to the mandatory design of services and/or products that protect consumer rights in the area of privacy throughout the life-cycle of the data. Thus, the text includes explicit measures for circumstances which may have been open to data processing abuse in the past. This set of measures means giving data subjects greater control over the publication and processing of data about themselves. By improving confidence in digital services, the intention is to increase people's predisposition to cede personal information, thus helping to generate value from the data.

The following are some of the requirements listed in the text:

(i) Article 5: This requires the inclusion of means for the data subject to exercise their rights (access, rectification, blocking, erasure and objection) effectively.

(ii) Recital 33 and Article 5: The minimum amount of data required to provide a service (even a free one) should be collected; should further information be needed for another purpose, the data subject must be given the option to refuse consent, without this refusal implying the withdrawal of the service.

(iii) Article 7: Consent for data processing should be obtained in such a way that it is clearly distinguished from other treatments, leaving no room for any kind of confusion. Thus, pre-ticked boxes to obtain this consent are not permitted.

(iv) Article 7: This requires it to be as easy to withdraw consent as it is to give it.

(v) Article 13a (new): This lays out standardised formats in which to present information to the data subject, with the manifest aim of increasing the transparency with which institutions handle personal data.

(vi) Article 23: This introduces the concept of data protection by design and default, with allusion to the

requirement that the results of impact assessment should be taken into account when developing data protection measures and procedures.
The adoption of these measures ***will require organisations to redesign many of their internal processes which are already processing personal data*** and which will be absolutely necessary if the data subject is to have real control over personal information.

Certifications

Another area which is developed in detail by the Parliament is addressed in Article 39: certifications. The revised text grants nationally monitored authorities the faculties to issue "European Data Protection Seals". These seals, which will be valid for five years at the most, will be issued to institutions which submit voluntarily to certification procedures, and they will ensure that personal data processing is carried out in compliance with the rule. In this context, the national supervisory authorities can certify third-party auditors to carry out the supervision and auditing procedures in the certification process.
The existence of these seals is particularly germane for those institutions which are weighing up whether to outsource part of their process or services in which personal data are processed, and most especially in the case of outsourcing services in the cloud. Subcontracting these services does not exempt the contracting company from responsibility for personal data processing and thus subcontracting services involves prior verification or, if pertinent, obliging the service provider to apply the safety measures laid down by the regulation. Data protection seals will help to provide guarantees and will make it simpler to choose suppliers, which is particularly helpful for start-ups and SMEs which start their business projects adopting public cloud service solutions.
It would be easier if specific guidelines were prepared by a competent European authority on how to implement these security measures in institutions; these guidelines would then be a reference for the supervisory agencies and the certified auditors.

Penalties

The Parliamentary review significantly toughens the sanctions, which can go up to EUR100mn or 5% of the offending institution's total turnover business volume (whichever is higher), compared to the EUR1mn, or 2% of business volume, recommended in the Commission's text. This is clearly an attempt to pressurise the technological giants to comply with European precepts, since the severity of the current penalties is not an obstacle to the development of their business strategies.
There is also a new addition: the option of carrying out regular audits on sanctioned institutions. This type of sanction is customary in North American regulations, but is new to Europe.

International data transfers

When it comes to international data transfer, the text continues to mandate specific authorisations for sending data to countries that have not been approved by the Commission, which according to article 43a (new), is responsible for conducting continuous supervision of new development in third countries. Nevertheless, the inclusion of article 43a (new) is important, insofar as it declares that rulings passed in other countries which require a controller or processor to make personal data public should not be recognised, unless permission has been obtained from the national data protection authority and the data subject has been previously informed that their information is going to be sent. This is a measure which has been designed in view of the cases of data being revealed by international firms headquartered in the United States to their government, which has provoked an international spying scandal. Even so, the way in which the text has been written does not make clear how to mediate the situation when the data processor collects data in the European Union, but is based in a third country. On the other hand, the scope of the regulation covers institutions which are not based in the Union which process data about European citizens (in exchange for payment or not), arising from a goods or services offering, or in order to track these data subjects.
In any event, the difficulties in applying these measures are many and will not be avoided without close international collaboration.

Assessment

The revised texts adopted for the proposed regulation by the Parliament introduce changes that endeavour to find a delicate balance between

protecting consumer rights and supporting innovation and development of data-based businesses.

Although perhaps not all aspects of data processing have been satisfactorily dealt with on all positions, a long regulatory process does not help either side and the community authorities have expressed the urgent need to approve this new legal framework.

In any event, still to come is the development of guidelines, instructions and recommendations, which are the responsibility of the European Data Protection Supervisor, and the development of proposals to review the applicable legal frameworks for specific personal data processes. With all these issues pending, European regulatory activity in the area of data protection will continue for the next few years.