1 General Data Protection Regulation

Main issues and impact on financial institutions

The new General Data Protection Regulation (GDPR) will further harmonize the EU framework for the processing of personal data. Financial institutions will have to adapt their internal processes to comply with the new Regulation, which follows a risk-based approach and fosters a culture of accountability.

Financial institutions are increasingly paying attention to the value they can extract from the large amounts of data they have access to: information self-reported by customers, transactional data that banks directly observe, internal operational data or information publicly available on the Internet. Big data and analytical techniques have opened a broad window of opportunities to increase revenues and reduce costs. By better knowing their customers, banks can anticipate their needs and offer them more tailored advice, products and services at the right time. Credit-risk assessment and fraud prevention may improve thanks to new analytics. Internal processes can be increasingly automatized and decision-making can be based on better evidence. Moreover, banks could provide intelligence services to third-parties, based on data analytics.

When analytics involve the use of personal data[1], regulation has much to say. Processing personal data is a highly regulated activity in most of the developed world, and particularly in the European Union (EU), where the 1995 Data Protection Directive set the general framework that has been in place until now. It will be replaced by the new General Data Protection Regulation (GDPR), a single set of rules directly applicable across the EU. This will further harmonize the EU regulatory framework, since national transpositions of the Directive have led to inconsistences between Member States.

After three years of intense negotiations, GDPR was finally adopted last month and will take effect two years after its formal publication.

Main issues in the new regulation

- The new Regulation creates a level playing field between firms established or not in the EU, since it extends its **scope** to organizations outside the Union when they offer goods or services to individuals in the Union or monitor their behaviour. Many of these organizations will need to appoint a representative in the EU. Moreover, data processors — not only controllers[2] — will be subject to direct obligations.
- The **consent** of the data subject remains the main legal basis for processing personal data. Yet obtaining it will be harder under GDPR, since it will have to be shown "by a statement or clear affirmative action", which closes the door for relying on "opt-out" mechanisms. The consent can be withdrawn, has to be specific to each data processing and the data controller is required to be able to demonstrate that consent was given.
- In the absence of consent, the "**legitimate interest**" of a controller may provide a legal basis for processing personal data, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. Although the existence of a legitimate interest requires specific assessment, the "whereas clauses" mention fraud prevention and marketing purposes as possible grounds for a legitimate interest.
- The **rights of the data subjects** will be reinforced. In particular, individuals will be entitled to receive the personal data concerning them and, when technically feasible, to have such data transmitted directly from one service provider to another (a "right to portability"). Moreover, the existing "right to be

1: The new General Data Protection Regulation (GDPR) defines personal data as "any information relating to an identified or identifiable natural person"
2: The 'controller' is the entity that determines the purposes and means of the processing of personal data, whereas the 'processor' is the one which processes personal data on behalf of the controller.

forgotten" — set by the EU Court of Justice — will be codified in the new regulation. When an individual no longer wants his/her data to be processed, and there are no legitimate grounds for retaining it, the controller shall have the obligation to erase said data. Moreover, when the personal data to be erased have been made public, the controller shall take reasonable steps to inform other controllers that are processing the data.

- In line with the principle of **accountability**, some formal requirements are removed, but controllers are obliged to implement appropriate technical and organisational measures and be able to demonstrate the compliance of their processing operations. In particular, controllers must conduct a data protection impact assessment for more risky processing operations; keep record of all processing activities under their responsibility and notify data breaches — depending on the risks involved — to supervisory authorities and data subjects. Moreover, companies processing sensitive data on a large scale or monitoring large amounts of personal data will have to appoint a Data Protection Officer (DPO), in charge of assisting the controller or processor to monitor internal compliance with the Regulation.
- To reduce the legal risk faced by firms under such a principles-based regulatory framework, GDPR will introduce **certification mechanisms**. Accredited certification bodies will be able to certify controllers and processors on the basis of the criteria approved by the supervisory authorities. A common 'European Data Protection Seal' could also be introduced by the newly created European Data Protection Board.
- The existing regime for **international data transfers** will remain with no significant changes. The main ways for allowing cross-border transfers will continue to be "adequacy decisions" — by which the Commission recognises that a third country ensures an adequate level of protection — or implementing appropriate safeguards, such as binding corporate rules or model contract clauses. GDPR will remove the need for prior authorisation when transfers are based on certain approved safeguards.
- National data protection authorities (DPAs) will be in charge of **supervising** the application of the Regulation. In cases of cross-border processing, the lead supervisory authority — the one of the main or the single establishment of the firm — and the other concerned authorities will have to cooperate. The newly created European Data Protection Board, composed of representatives of the national DPAs and the European Data Protection Supervisor, will be in charge of ensuring consistency and will be competent to take binding decisions in case of disputes between supervisory authorities from different Member States.
- GDPR sets the maximum **administrative fines** that data protection authorities shall impose to controllers or processors in case of infringement. The most severe of these (e.g. breach of the conditions for consent or the requirements for international transfers) will be subject to fines up to 4% of total annual worldwide turnover or 20 million euros, whichever is higher.

Impact on financial services

Financial institutions will have to adapt their internal processes to meet the new requirements for obtaining consent; ensure data subjects can exercise their new rights; identify risky operations; improve traceability of all processing operations; and streamline the mechanisms to notify breaches. This will involve significant compliance costs. Moreover, given the risk-based approach of the new Regulation, firms are expected to rely on certification mechanisms to reduce the legal risk they face.

Finally, by further harmonizing the EU regulatory framework, GDPR should contribute to strengthen the Single Market for retail financial services, as intended by the ongoing European Commission's Green Paper. However, reaching an effective harmonization depends on the cooperation between all national DPAs and on the role of the European Data Protection Board to ensure consistency.

DISCLAIMER

This document has been prepared by BBVA Research Department, it is provided for information purposes only and expresses data, opinions or estimations regarding the date of issue of the report, prepared by BBVA or obtained from or based on sources we consider to be reliable, and have not been independently verified by BBVA. Therefore, BBVA offers no warranty, either express or implicit, regarding its accuracy, integrity or correctness.

Estimations this document may contain have been undertaken according to generally accepted methodologies and should be considered as forecasts or projections. Results obtained in the past, either positive or negative, are no guarantee of future performance.

This document and its contents are subject to changes without prior notice depending on variables such as the economic context or market fluctuations. BBVA is not responsible for updating these contents or for giving notice of such changes.

BBVA accepts no liability for any loss, direct or indirect, that may result from the use of this document or its contents.

This document and its contents do not constitute an offer, invitation or solicitation to purchase, divest or enter into any interest in financial assets or instruments. Neither shall this document nor its contents form the basis of any contract, commitment or decision of any kind.

In regard to investment in financial assets related to economic variables this document may cover, readers should be aware that under no circumstances should they base their investment decisions in the information contained in this document. Those persons or entities offering investment products to these potential investors are legally required to provide the information needed for them to take an appropriate investment decision.

This report has been produced by the Digital Regulation Unit:

Chief Economist for Digital Regulation Unit
Álvaro Martín
alvaro.martin@bbva.com

Vanesa Casadas
vanesa.casadas@bbva.com

Israel Hernanz
israel.hernanz@bbva.com

Alicia Sánchez
alicia.sanchezs@bbva.com

Javier Sebastián
jsebastian@bbva.com

Pablo Urbiola
pablo.urbiola@bbva.com

With the contribution of:

Francisco Borja Larrumbide Martínes
fborja.larrumbide@bbva.com

Alfonso Arellano
alfonso.arellano.espinar@bbva.com

BBVA Research

Group Chief Economist
Jorge Sicilia Serrano

Developed Economies Area
Rafael Doménech
r.domenech@bbva.com

Spain
Miguel Cardoso
miguel.cardoso@bbva.com

Europe
Miguel Jiménez
mjimenezg@bbva.com

US
Nathaniel Karp
Nathaniel.Karp@bbva.com

Emerging Markets Area

Cross-Country Emerging Markets Analysis
Alvaro Ortiz
alvaro.ortiz@bbva.com

Asia
Le Xia
le.xia@bbva.com

Mexico
Carlos Serrano
carlos.serranoh@bbva.com

Turkey
Alvaro Ortiz
alvaro.ortiz@bbva.com

LATAM Coordination
Juan Manuel Ruiz
juan.ruiz@bbva.com

Argentina
Gloria Sorensen
gsorensen@bbva.com

Chile
Jorge Selaive
jselaive@bbva.com

Colombia
Juana Téllez
juana.tellez@bbva.com

Peru
Hugo Perea
hperea@bbva.com

Venezuela
Julio Pineda
juliocesar.pineda@bbva.com

Financial Systems and Regulation Area
Santiago Fernández de Lis
sfernandezdelis@bbva.com

Financial Systems
Ana Rubio
arubiog@bbva.com

Financial Inclusion
David Tuesta
david.tuesta@bbva.com

Regulation and Public Policy
María Abascal
maria.abascal@bbva.com

Digital Regulation
Álvaro Martín
alvaro.martin@bbva.com

Global Areas

Economic Scenarios
Julián Cubero
juan.cubero@bbva.com

Financial Scenarios
Sonsoles Castillo
s.castillo@bbva.com

Innovation & Processes
Oscar de las Peñas
oscar.delaspenas@bbva.com

Contact details:

Azul Street, 4
La Vela Building - 4 and 5 floor
28050 Madrid (Spain)
Tel.: +34 91 374 60 00 and +34 91 537 70 00
Fax: +34 91 374 30 25
bbvaresearch@bbva.com
www.bbvaresearch.com