

1 Reglamento General de Protección de Datos

Aspectos principales e impacto en las instituciones financieras

El nuevo Reglamento General de Protección de Datos (GDPR por sus siglas en inglés) armonizará más el marco de la UE para el tratamiento de datos personales. Las instituciones financieras tendrán que adaptar sus procesos internos para cumplir con la nueva regulación, que presenta un enfoque basado en el riesgo y fomenta una cultura de responsabilidad en las empresas.

Las instituciones financieras cada vez prestan más atención al valor que pueden extraer de la gran cantidad de datos que tienen a su alcance: información proporcionada por los clientes, datos transaccionales, datos de la operativa interna o información disponible públicamente en Internet. El *big data* y las técnicas de análisis han abierto una amplia ventana de oportunidades para aumentar los ingresos y reducir los costes. Al conocer mejor a los clientes, los bancos pueden anticiparse a sus necesidades y ofrecerles asesoramiento, productos y servicios más personalizados en el momento oportuno. La evaluación del riesgo crediticio y la prevención del fraude también pueden mejorar gracias a los nuevos análisis. Los procesos internos pueden automatizarse cada vez más y la toma de decisiones puede basarse en mejor evidencia. Además, los bancos podrían prestar servicios de inteligencia a terceros basados en el análisis de datos.

Cuando el análisis incluye el uso de datos personales¹, la regulación tiene mucho que decir. El tratamiento de datos personales es una actividad muy regulada en la mayor parte del mundo desarrollado, y especialmente en la Unión Europea, donde la Directiva sobre Protección de Datos de 1995 estableció el marco general que ha estado vigente hasta ahora. Dicha Directiva será sustituida por el nuevo Reglamento General de Protección de Datos (GDPR por sus siglas en inglés), un solo conjunto de normas de aplicación directa en toda la UE. De esta forma se armonizará más el marco regulatorio de la UE, pues las transposiciones nacionales de la Directiva han dado lugar a inconsistencias entre los estados miembros.

Tras años de intensas negociaciones, GDPR se adoptó finalmente el mes pasado y entrará en vigor dos años después de su publicación formal.

Aspectos principales del nuevo Reglamento

- Se crean unas reglas de juego uniformes entre empresas establecidas o no en la UE, pues el nuevo Reglamento amplía su **alcance** a las organizaciones que están fuera de la Unión pero ofrecen bienes o servicios a particulares de la UE o monitorizan su comportamiento. Muchas de estas organizaciones tendrán que nombrar un representante en la UE. Además, los procesadores de datos, no solo los controladores², estarán sujetos a obligaciones directas.
- El **consentimiento** del interesado seguirá siendo la principal base legal para el tratamiento de datos personales, pero la obtención de dicho consentimiento será más ardua en virtud de GDPR, pues tendrá que demostrarse "mediante una acción afirmativa clara", lo que cierra la puerta al uso del consentimiento tácito. El consentimiento puede retirarse, tiene que ser específico para cada procesamiento de datos personales y el controlador debe poder demostrar que el interesado dio consentimiento.
- En ausencia de consentimiento, el "**interés legítimo**" de un controlador puede servir de base legal para procesar datos personales, siempre que no prevalezcan los intereses o los derechos y libertades del interesado. Aunque la existencia de un interés legítimo requiere una evaluación específica, los

1: GDPR define datos personales como "toda información relativa a una persona física identificada o identificable".

2: El "controlador" es la entidad que determina los fines y medios del tratamiento de datos personales, mientras que el "procesador" es la entidad que procesa los datos personales en nombre del controlador.

"considerandos" del Reglamento mencionan la prevención del fraude y los fines de mercadotecnia directa como posibles bases de un interés legítimo.

- Los **derechos de los titulares de los datos** se reforzarán. En particular, las personas tendrán derecho a recibir los datos personales que les conciernen y, cuando sea técnicamente factible, a que dichos datos se transmitan directamente de un proveedor de servicios a otro ("derecho de portabilidad"). Además, el ya existente "derecho al olvido", establecido por el Tribunal de Justicia de la Unión Europea, se codifica en el nuevo Reglamento. Si una persona ya no desea que sus datos se procesen y no hay base legítima para retenerlos, el controlador tendrá la obligación de borrar dichos datos. Además, cuando los datos personales a borrar se hayan hecho públicos, el controlador deberá tomar medidas razonables para informar a los otros controladores que están tratando los datos.
- En línea con el principio de **responsabilidad**, se eliminan requisitos formales, pero los controladores están obligados a implementar las medidas técnicas y organizativas adecuadas y tienen que ser capaces de demostrar que sus operaciones de tratamiento de datos cumplen con el Reglamento. En particular, los controladores deben llevar a cabo una evaluación de impacto para las operaciones de mayor riesgo, mantener un registro de todas las actividades de tratamiento de datos bajo su responsabilidad y notificar las violaciones de datos personales —en función de los riesgos— a las autoridades supervisoras y a los individuos afectados. Además, las empresas que procesan datos sensibles a gran escala o que monitorizan grandes cantidades de datos personales tendrán que nombrar un Delegado de Protección de Datos que se encargará de ayudar a la empresa a supervisar el cumplimiento interno del Reglamento.
- Para reducir el riesgo legal al que se enfrentan las empresas en un marco regulatorio basado en principios, GDPR introducirá **mecanismos de certificación**. Los organismos acreditados podrán certificar a los controladores y procesadores basándose en los criterios aprobados por las autoridades supervisoras. El recién creado Consejo Europeo de Protección de Datos también podría introducir un "Sello Europeo de Protección de Datos".
- El régimen existente para las **transferencias de datos internacionales** se mantendrá sin cambios importantes. Los principales mecanismos para que se permitan las transferencias seguirán siendo las "decisiones de adecuación" mediante las cuales la Comisión reconoce que un tercer país garantiza un nivel de protección adecuado, o la implementación de garantías adecuadas, como normas corporativas vinculantes o cláusulas estándar en los contratos. GDPR eliminará la necesidad de autorización previa cuando las transferencias se basen en determinadas garantías reconocidas por las autoridades.
- Las autoridades nacionales de protección de datos se encargarán de **supervisar** la aplicación del Reglamento. En los casos de procesamiento transfronterizo, la autoridad supervisora principal (la del país en el que está el establecimiento único o el establecimiento principal de la empresa) y las otras autoridades afectadas tendrán que cooperar. El recién creado Comité Europeo de Protección de Datos, compuesto por representantes de las autoridades nacionales y por el Supervisor Europeo de Protección de Datos, se encargará de garantizar la coherencia y será competente para tomar decisiones vinculantes en caso de disputa entre las autoridades de distintos estados miembros.
- GDPR establece las **sanciones administrativas** máximas que las autoridades de protección de datos impondrán a los controladores o procesadores en caso de infracción. Las infracciones más graves (como el incumplimiento de las condiciones para el consentimiento o de los requisitos para las transferencias internacionales) estarán sujetas a multas de hasta el 4% de la facturación mundial anual o 20 millones de euros, la cantidad que sea más elevada.

Impacto en los servicios financieros

Las instituciones financieras tendrán que adaptar sus procesos internos para cumplir con los nuevos requisitos para obtener consentimiento, asegurarse de que los sujetos a los que pertenecen los datos pueden ejercer sus nuevos derechos, identificar las operaciones de mayor riesgo, mejorar la trazabilidad de todas las operaciones de tratamiento de datos y optimizar los mecanismos para notificar las violaciones de datos personales. Esto conllevará importantes costes de cumplimiento. Además, dado el enfoque basado en el riesgo del nuevo Reglamento, se espera que las empresas recurran a los mecanismos de certificación para reducir el riesgo legal al que se enfrentan.

Por último, al armonizar más el marco regulatorio de la UE, GDPR debería contribuir a fortalecer el Mercado Único de servicios financieros minoristas, tal y como pretende el Libro Verde de la Comisión Europea. No obstante, conseguir una verdadera armonización depende de la cooperación entre todas las autoridades de protección de datos nacionales y del papel del Comité Europeo de Protección de Datos para garantizar la coherencia en las interpretaciones.

AVISO LEGAL

El presente documento, elaborado por el Departamento de BBVA Research, tiene carácter divulgativo y contiene datos, opiniones o estimaciones referidas a la fecha del mismo, de elaboración propia o procedentes o basadas en fuentes que consideramos fiables, sin que hayan sido objeto de verificación independiente por BBVA. BBVA, por tanto, no ofrece garantía, expresa o implícita, en cuanto a su precisión, integridad o corrección.

Las estimaciones que este documento puede contener han sido realizadas conforme a metodologías generalmente aceptadas y deben tomarse como tales, es decir, como previsiones o proyecciones. La evolución histórica de las variables económicas (positiva o negativa) no garantiza una evolución equivalente en el futuro.

El contenido de este documento está sujeto a cambios sin previo aviso en función, por ejemplo, del contexto económico o las fluctuaciones del mercado. BBVA no asume compromiso alguno de actualizar dicho contenido o comunicar esos cambios.

BBVA no asume responsabilidad alguna por cualquier pérdida, directa o indirecta, que pudiera resultar del uso de este documento o de su contenido.

Ni el presente documento, ni su contenido, constituyen una oferta, invitación o solicitud para adquirir, desinvertir u obtener interés alguno en activos o instrumentos financieros, ni pueden servir de base para ningún contrato, compromiso o decisión de ningún tipo.

Especialmente en lo que se refiere a la inversión en activos financieros que pudieran estar relacionados con las variables económicas que este documento puede desarrollar, los lectores deben ser conscientes de que en ningún caso deben tomar este documento como base para tomar sus decisiones de inversión y que las personas o entidades que potencialmente les puedan ofrecer productos de inversión serán las obligadas legalmente a proporcionarles toda la información que necesiten para esta toma de decisión.

El contenido del presente documento está protegido por la legislación de propiedad intelectual. Queda expresamente prohibida su reproducción, transformación, distribución, comunicación pública, puesta a disposición, extracción, reutilización, reenvío o la utilización de cualquier naturaleza, por cualquier medio o procedimiento, salvo en los casos en que esté legalmente permitido o sea autorizado expresamente por BBVA.

Este informe ha sido elaborado por la unidad de Regulación Digital:

Economista Jefe de Regulación Digital

Álvaro Martín
alvaro.martin@bbva.com

Vanesa Casadas
vanesa.casadas@bbva.com

Pablo Urbiola
pablo.urbiola@bbva.com

Israel Hernanz
israel.hernanz@bbva.com

Alicia Sánchez
alicia.sanchezs@bbva.com

Javier Sebastián
jsebastian@bbva.com

Con la colaboración de:

Francisco Borja Larrumbide Martínez
fborja.larrumbide@bbva.com

Alfonso Arellano
alfonso.arellano.espinar@bbva.com

BBVA Research

Economista Jefe Grupo BBVA

Jorge Sicilia Serrano

Área de Economías Desarrolladas

Rafael Doménech
r.domenech@bbva.com

España

Miguel Cardoso
miguel.cardoso@bbva.com

Europa

Miguel Jiménez
mjimenezg@bbva.com

Estados Unidos

Nathaniel Karp
Nathaniel.Karp@bbva.com

Área de Economías Emergentes

Análisis Transversal de Economías

Emergentes
Álvaro Ortiz
alvaro.ortiz@bbva.com

Asia

Le Xia
le.xia@bbva.com

México

Carlos Serrano
carlos.serranoh@bbva.com

Turquía

Álvaro Ortiz
alvaro.ortiz@bbva.com

Coordinación LATAM

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

Perú

Hugo Perea
hperea@bbva.com

Venezuela

Julio Pineda
juliocesar.pineda@bbva.com

Área de Sistemas Financieros y Regulación

Santiago Fernández de Lis
sfernandezdelis@bbva.com

Sistemas Financieros

Ana Rubio
arubiog@bbva.com

Inclusión Financiera

David Tuesta
david.tuesta@bbva.com

Regulación y Políticas Públicas

María Abascal
maria.abascal@bbva.com

Regulación Digital

Álvaro Martín
alvaro.martin@bbva.com

Áreas Globales

Escenarios Económicos

Julián Cubero
juan.cubero@bbva.com

Escenarios Financieros

Sonsoles Castillo
s.castillo@bbva.com

Innovación y Procesos

Oscar de las Peñas
oscar.delaspenas@bbva.com

Interesados dirigirse a:

BBVA Research

Calle Azul, 4
Edificio de la Vela - 4ª y 5ª plantas
28050 Madrid (España)
Tel.: +34 91 374 60 00 y +34 91 537 70 00
Fax: +34 91 374 30 25
bbvaresearch@bbva.com
www.bbvaresearch.com