

# El camino a la generación de valor

*Creación de un activo de datos gobernado y sostenible para el GDPR y más allá*



# 1. El GDPR como oportunidad de negocio

Con la introducción del Reglamento General de Protección de datos (GDPR) y su aplicación a partir del 25 de mayo de 2018, se creará un nuevo equilibrio entre los intereses comerciales y los derechos de los consumidores en torno a los datos personales y confidenciales. Todas las personas poseen datos personales que tienen que compartir con empresas – clientes durante transacciones, empleados en el trabajo, business partners en un contrato. La interacción positiva y responsable con todos estos interesados es el objetivo del Reglamento, así como garantizar que el negocio sea sostenible y capaz de seguir innovando.

En el periodo previo a su aplicación, se lanzarán muchas iniciativas para informar a las personas sobre sus derechos y a las empresas sobre la necesidad de tratar sus datos. Por el momento, el nivel de concienciación es bajo – solo el 10% de los consumidores encuestados afirmó conocer perfectamente el GDPR (Fuente: “GDPR Impact 2017”, DataIQ encargó una encuesta a 1.001 consumidores británicos, realizada por Research Now, febrero de 2017). Pero la protección de datos pasará a ser de interés general, igual que sucedió con la seguridad de los datos. La diferencia reside en la oportunidad de demostrar las ventajas de compartir datos, en lugar de protegerse ante las consecuencias de una infracción de datos.

Las principales organizaciones basadas en datos están creando un nuevo enfoque al intercambio de datos-valor, que permite otorgar control y acceso a los interesados, al tiempo que se da soporte a los principales procesos de negocio con flujos de

datos gobernados y sostenibles. El GDPR requiere una revisión del tratamiento de datos integral, que favorezca tanto a los interesados como al negocio.

La adopción de este enfoque positivo puede ayudar a crear valor para el negocio en dos dimensiones:

**Valor de marca** – a medida que las personas conozcan sus nuevos derechos, se dirigirán a las marcas que ofrezcan la mejor experiencia y cumplimiento. Como consecuencia, los líderes pueden ganar confianza y ventaja comercial.

**Valor de negocio** – al agilizar las políticas de datos, introducir un tratamiento de datos más eficiente e integrado y garantizar que los sistemas operativos están en consonancia con el GDPR, la empresa puede generar ahorros.



## 2. GDPR – diseñado sobre una base sólida

Cuando entre en vigor el GDPR, se cumplirán 20 años desde que se presentó la Directiva de protección de datos. En aquel momento, todo había cambiado – los tipos de datos creados, los procesos utilizados para recopilarlos y controlarlos, los sistemas utilizados para su gestión, análisis y despliegue. Las organizaciones que ya respetan los principios de esta normativa estarán en mejores condiciones de adaptarse al Reglamento, aunque deberán prestar especial atención a las ampliaciones y mejoras que presenta.



### Los datos son más personales –

El GDPR amplía la definición de datos personales, cubriendo casi todo lo que pueda identificar a una persona, como datos sobre dónde está (ubicación), qué contenido o apps consume (comportamiento), qué dispositivo utiliza (ID de dispositivo). También será necesario controlar los datos no estructurados, como comentarios de clientes, revisiones, publicaciones en blogs, notas al servicio al cliente e incluso mensajería interna.



### Responsabilidad completa –

además de respetar el GDPR como organización, los controladores de datos deben validar que sus business partners (procesadores de datos) también cumplan el Reglamento. Ambas partes conllevan obligaciones para garantizar la seguridad de los datos, y nuevos deberes relativos a la notificación de infracciones de datos.



### Más acceso y consentimiento –

además de los derechos vigentes, como acceso y rectificación, se amplían los derechos individuales, incluyendo la capacidad de revocar el consentimiento, mover los datos a otro proveedor o solicitar su supresión.



### Nuevas obligaciones de datos –

se introducen nuevos requisitos, a destacar la obligación de contar con un Delegado de Protección de Datos, así como la adopción de nuevas estrategias de gobierno de datos y un enfoque basado en riesgos.



### Europeo, en cualquier lugar –

se garantiza la protección de estos derechos a cualquier ciudadano de la Unión Europea, independientemente de dónde residan o se traten sus datos. Si los datos se transfieren fuera de la UE, estos derechos se mantienen. Las transferencias de datos personales entre territorios deben realizarse con sumo cuidado.



### Cumplimiento más estricto –

se otorgan más poderes a las autoridades encargadas de la protección de datos para garantizar el cumplimiento del GDPR, especialmente la capacidad de imponer una sanción de hasta el 4% de la facturación global anual o 20 millones de euros, el que sea de importe superior.



### 3. Pasos claves en el camino a la generación de valor

La finalidad del GDPR es lograr un mayor equilibrio entre los intereses legítimos del negocio y los derechos de las personas individuales. Abordar esta cuestión a través de un enfoque creativo y transparente es la clave para cubrir las nuevas demandas del Reglamento y para identificar nuevo valor de un activo de datos gobernado y sostenible.

IBM ha identificado cinco pasos clave que las organizaciones deberían tener en cuenta:

**Gobierno** – una clave del GDPR es la participación interdisciplinaria en el modo de capturar, tratar, gestionar, proteger y desplegar datos personales. La estrategia inicial consiste en la adopción de Privacidad por diseño en el desarrollo de nuevos procesos dependientes de los datos, junto con Evaluaciones del impacto de la privacidad para identificar riesgos y la exposición de cualquier elemento de datos sensibles.

Explicar a los usuarios de modo claro y transparente por qué se necesitan sus datos, cómo se utilizarán y gestionarán y por cuánto tiempo requerirá revisar los avisos de privacidad. Las aprobaciones y consentimientos específicos deberán registrarse. El responsable del control en toda la organización será la figura del Delegado de protección de datos (DPO), que dispondrá de responsabilidades, rango y soporte específicos. Los roles existentes pueden ocupar este cargo, con formación adicional, o bien será necesaria una nueva contratación. Como alternativa más económica, se puede subcontratar un DPO compartido.

En este gobierno también pueden entrar terceros, como procesadores de datos, siempre y cuando se valide que estos business partners se rigen por el GDPR y así quede reflejado y detallado en todos los acuerdos contractuales.

**Derechos y procesos** – la ampliación de los derechos de los interesados, como la revocación del consentimiento, portabilidad y supresión, junto con sus derechos actuales, como la rectificación y solicitudes de acceso, puede requerir desarrollo adicional para garantizar su integridad. Las soluciones técnicas serán claves en este proceso, así como las estrategias revisadas.

Es posible que también sea necesario adaptar los procesos de negocio para prepararlos para el GDPR. Funciones de primera línea, como la gestión de la relación con el cliente, tan dependientes de los datos personales, tendrán que revisarse y rediseñarse, en caso necesario. Funciones de back office, como

los recursos humanos, también tendrán que ajustarse para dar soporte a los derechos de los empleados y evitar riesgos generados por datos personales no controlados.

**Datos** – los datos circulan entre organizaciones, procedentes de todos los procesos y canales de negocio, así como de fuentes externas, a través del marketing digital, socios de distribución y otros puntos de contacto del mercado. Si su modelo de negocio se basa fundamentalmente en esta circulación de información personal, deberá contar con un programa de auditoría y descubrimiento de datos. Correlacionar qué tipos de datos se utilizan, dónde se almacenan y si son sensibles marcará el camino a seguir para cumplir con el GDPR.

La integración de todos estos conjuntos para crear una vista de 360 grados será una condición esencial. Una única vista del cliente garantiza que cada uno pueda acceder, corregir o extraer sus datos personales, como establece el Reglamento, además de formar la base para la futura creación de valor a partir de los datos. También optimiza la gestión del ciclo de vida de la información, incluyendo, si se solicita legítimamente, la eliminación del registro de un cliente.

**Seguridad de los datos** – mantener la seguridad de la información personal es clave en el imperativo de la protección de datos. Del mismo modo que se protege un activo de negocio valioso, la seguridad de los datos también es vital para los clientes, que cada vez están más preocupados por los riesgos personales de una infracción o pérdida de datos. Invertir en la seguridad de los datos adecuada puede ser un diferenciador competitivo en la era post-GDPR de relaciones basadas en la confianza.

Probablemente una de las mayores exigencias del GDPR será notificar al regulador cualquier infracción de datos en un plazo de 72 horas desde su detección, y avisar a las personas afectadas en un periodo de tiempo razonable. La adopción de una gestión de acceso a datos estándar del sector y herramientas de supervisión de seguridad, además de una mayor coordinación de la capacidad de respuesta ante incidentes, ayuda a prepararse para esta obligación.



**Personas y comunicaciones** – la dimensión humana de prepararse para el GDPR demanda una combinación de comunicaciones formales y refuerzo constante. Los mensajes por roles y las comunicaciones empresariales deben detallar las nuevas prácticas de trabajo y las pautas de la nueva cultura organizativa.

El personal debe comprender la necesidad de tratar la información personal como un activo vital y de respetar los derechos de las personas sobre sus datos, lo que quizá requiera formación y refuerzo continuo. Los programas de formación, especialmente los proporcionados como servicio, deben basarse en el programa del GDPR.

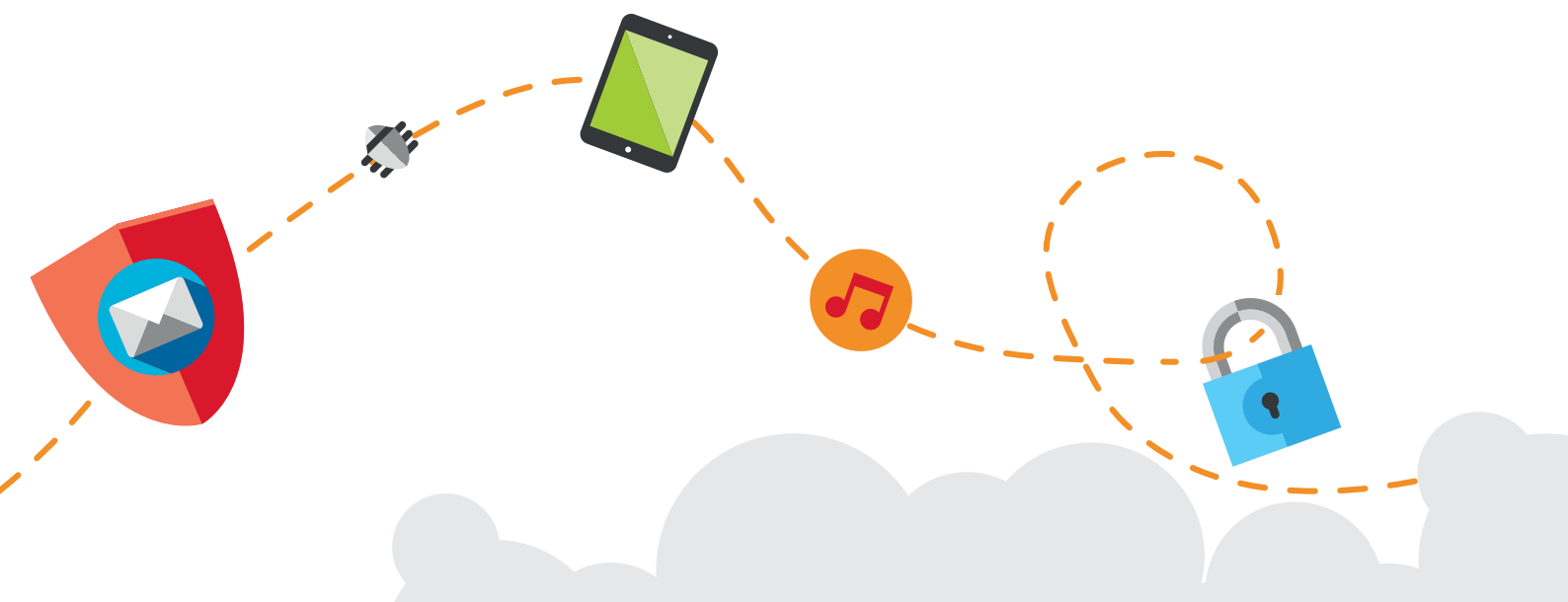
## 4. IBM como guía en todo el trayecto

IBM ofrece asistencia en el programa de preparación para el GDPR mediante una solución completa. Nuestros conocimientos en servicios de negocio globales, así como nuestras tecnologías e innovaciones en torno a la gestión de la privacidad, le ayudarán a preparar su negocio.

Además, nosotros realizamos el mismo trayecto. IBM está ejecutando su propio proyecto GDPR, y podemos compartir la información y los conocimientos de nuestra experiencia directa, así como los factores de éxito que hemos aprendido dando soporte a nuestros clientes.

- **Asesores con experiencia** – expertos en la materia con un gran conocimiento sobre protección de datos.
- **Gestión de cambios de negocio** – capital intelectual, recursos y herramientas para transformar procesos de negocio.

- **Soluciones tecnológicas** – desde la gestión de datos y la gestión del ciclo de vida de la información hasta la seguridad de la información y los informes de incidentes.
- **Oferta integral** – centrada en los cambios críticos que deben implementarse de cara al 25 de mayo de 2018, así como la generación de valor a largo plazo.





## Información adicional

Para obtener más información sobre el GDPR y cómo las soluciones de IBM le ayudan a proteger, controlar y conocer sus datos, póngase en contacto con un representante de IBM o bien visite:

[ibm.com/es-es/gdpr/](http://ibm.com/es-es/gdpr/)

© Copyright IBM Corporation 2017

IBM España  
Santa Hortensia 26  
28002 Madrid

Producido en España  
Junio de 2017  
Reservados todos los derechos.

IBM, el logotipo de IBM, [ibm.com](http://ibm.com) e IBM Watson son marcas registradas de International Business Machines Corporation en Estados Unidos y otros países. Otros nombres de productos y servicios pueden ser marcas registradas de IBM u otras empresas.

Las referencias a otros productos y servicios de IBM en esta publicación no implican que IBM tenga previsto ofrecerlos en todos los países en los cuales opera.

Aviso: Los clientes son responsables de garantizar el cumplimiento con las leyes y normativas aplicables, incluyendo el Reglamento General de Protección de Datos de la Unión Europea. Los clientes son los únicos responsables de obtener asesoramiento legal competente referente a la identificación y la interpretación de cualquier ley relevante que pudiera afectar a su negocio, así como cualquier medida que debieran tomar para su cumplimiento. Los productos, servicios y otras funcionalidades descritas en este documento no son los indicados para todas las situaciones del cliente y podrían estar sujetas a disponibilidad. IBM no proporciona asesoramiento legal, de contabilidad ni de auditoría, ni representa ni garantiza que sus servicios o productos son garantía de que los clientes cumplen con las leyes o normativas vigentes.



Recicle este documento