Grant Thornton

Riesgo

Regulación

Ciber seguridad

El Reglamento General de Protección de Datos (RGPD)

Prepare a su empresa para el RGPD

Octubre 2017

Índice

¿Qué es el RGPD y qué cambia?

El Reglamento General de Protección de Datos (RGPD) es la nueva ley de protección de datos de la Unión Europea (UE) que entrará en vigor el 25 de mayo de 2018.

Se va a aplicar en toda la UE, regirá a todas las empresas que operen en la Unión e incorporará un enfoque más coherente de protección de datos. Las empresas que operen con empresas con sede en la UE también se verán afectadas y deberán saber qué va a cambiar y cómo respetar la nueva legislación.

Las multas por incumplirlo pueden alcanzar ahora los 20 millones de euros o el 4% de la facturación global anual (la cifra que sea más alta).

¿Por qué se cambia la legislación sobre protección de datos?

Desde 1995, la Directiva de protección de datos (Directiva 95/46/CE) ha establecido cómo se protegen los datos de carácter personal dentro de la UE. No obstante, desde su aprobación, se han producido grandes avances en la sofisticación y volumen de creación y recopilación de datos; por ejemplo, con la aparición de las redes sociales, los servicios de cloud computing y la geolocalización. Puesto que la directiva es anterior a estos avances, ya no es adecuada para regir el actual panorama de datos; necesita renovarse para afrontar las preocupaciones actuales relativas a la privacidad y facilitar la coherencia en toda la UE. Esto es lo que va a hacer el RGPD.

El nuevo reglamento introduce una amplia serie de cambios. En el trasfondo de estos cambios está el esfuerzo continuo de la UE por proteger a sus ciudadanos y su información privada. El RGPD establecerá nuevos derechos para las personas y reforzará las protecciones actuales aplicando requisitos más estrictos a la forma en que las empresas utilizan los datos de carácter personal. Si lo incumplen, las sanciones serán mucho mayores.

¿Qué supone esto para su empresa?

El RGPD es una valiosa oportunidad para entender los datos de su empresa y utilizarlos de forma más eficaz. Sin embargo, exige un respeto estricto del nuevo reglamento y entender bien los cambios para evitar grandes multas.

En primer lugar, es fundamental ser consciente de que el RGPD anula y reemplaza todas las leyes de protección de datos existentes e incrementa las obligaciones de las empresas en materia de protección de datos y su responsabilidad en caso de incumplimiento. Asimismo, se aplica a todo el espectro de la gestión de datos: desde la recopilación de datos de carácter personal hasta su uso y eliminación. Su organización deberá implantar políticas y procedimientos que garanticen la supervisión de sus controles del RGPD y la documentación de su cumplimiento.

Las nuevas normas se aplican a las organizaciones que, con independencia de su tamaño, procesen datos de carácter personal. Se dedique a lo que se dedique su organización, el RGPD va a tener un impacto significativo. Puesto que la fecha de aplicación se está acercando, es fundamental prepararse con antelación.

Todas las organizaciones globales, tanto las de la UE como las que operan con empresas de la UE, deberán cumplir el RGPD a partir de mayo de 2018.

Entender los principales cambios

El RGPD introducirá amplios cambios que requieren la comprensión, aceptación interna entre las partes interesadas, y su preparación y aplicación adecuadas en toda la empresa. A continuación abordamos algunos de los principales cambios a modo de introducción general.

Mayores derechos para los titulares de los datos
El mayor cambio es que las personas se beneficiarán de unos derechos ampliados, por ejemplo, el derecho a oponerse a ciertos tipos de elaboración de perfiles y tomas de decisiones automatizadas. La necesidad de obtener un consentimiento también será más rigurosa. El consentimiento deberá ser explícito y afirmativo, tendrá que otorgarse con una finalidad específica y deberá ser sencillo retirarlo. Los interesados también pueden solicitar que los datos de carácter personal se borren o eliminen si no hay un motivo convincente para su procesamiento continuado.

Mayor obligación de rendir cuentas
Las organizaciones tendrán responsabilidades y obligaciones mayores. Tendrán que publicar avisos de procesamiento correcto más detallados en los que informen a los interesados de sus derechos en esta materia, les expliquen cómo se va a utilizar su información y especifiquen durante cuánto tiempo. Además, el nuevo reglamento incorpora el concepto de protección de la intimidad desde el diseño, lo que significa que las organizaciones deben diseñar la protección de datos para integrarla en nuevos procesos y sistemas empresariales.

Procesos formales de gestión de riesgos
Las organizaciones deben identificar formalmente los nuevos riesgos para la privacidad, en particular aquellos relacionados con los nuevos proyectos o en los que haya actividades relevantes de procesamiento de datos. Asimismo, deben conservar registros de sus actividades de procesamiento y crear inventarios internos. En el caso de las actividades de procesamiento de datos de alto riesgo, las Evaluaciones de Impacto relativas a la Protección de Datos (EIPD) serán obligatorias. También será obligatorio nombrar un Responsable de la Protección de Datos (RPD).

Notificación de infracciones de los datos
En el marco de los cambios para exigir una mayor rendición de cuentas, la notificación de las infracciones de los datos será más estricta. Si se produce una infracción importante de los datos, esta debe notificarse a la autoridad responsable de la protección de datos en un plazo de 72 horas y, en algunos casos, a la persona afectada sin retrasos indebidos.

Sanciones significativas
Las multas por incumplir el RGPD aumentarán considerablemente, hasta los 10 millones de euros o el 2% de la facturación global anual (la cifra que sea más alta) en el caso de las infracciones menores o técnicas, y hasta los 20 millones o el 4% de la facturación en el caso de carencias operativas más graves.

Requisitos para el procesamiento de los datos
El reglamento también impone nuevos requisitos a los procesadores de datos e incluye elementos que deberán ser contemplados en los contratos entre los procesadores de datos y los controladores.

Principales características del RGPD:

Mayores derechos para los titulares de datos
El derecho a rechazar ciertos tipos de elaboración de perfiles y tomas de decisiones automatizadas, y a solicitar que los datos de carácter personal innecesarios sean borrados.

Mayores obligaciones para las organizaciones
Como la publicación de avisos de procesamiento correcto más detallados, en los que informen a los interesados de sus derechos en esta materia,

Requisitos de consentimiento más estrictos
El consentimiento deberá ser explícito, libremente expresado para una finalidad específica y sencillo de retirar.

Notificación más estricta de infracciones
Las Infracciones de datos relevantes deben ser notificadas a los reguladores en un plazo de 72 horas y en ocasiones también al interesado.

Mayores evaluaciones del impacto sobre la privacidad
Las organizaciones deben identificar formalmente los nuevos riesgos para la privacidad, en particular en los nuevos proyectos.

Protección de la intimidad desde el diseño
Las organizaciones deben diseñar la protección de datos para integrarla en procesos y sistemas empresariales nuevos y antiguos.

Mayor conservación de la información
Las organizaciones deben conservar registros de las actividades de procesamiento realizadas, con DPIA obligatorias cuando se procesen datos de alto riesgo.

Multas significativas
La posible cuantía de las multas en caso de incumplimiento será considerable, pudiendo alcanzar los 20 millones de euros o el 4% de la facturación (la cifra que sea más alta).

Nombramiento de RPD
El nombramiento de un Responsable de Protección de Datos será obligatorio para muchas organizaciones.

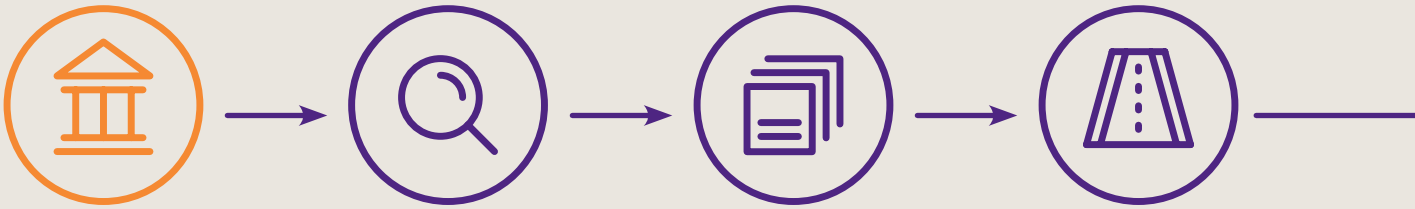
Mayor alcance regulatorio
El nuevo reglamento se aplicará tanto al controlador de datos como al procesador.

¿Cómo preparar a su empresa?

El panorama jurídico de la protección de datos evoluciona rápidamente y supone desafíos para las empresas, los gobiernos y las autoridades públicas. Si su organización está orientada a los consumidores, opera en el entorno *online*, en el sector de servicios financieros o posee datos de carácter personal sensibles, puede verse especialmente afectada.

Se aproxima la fecha de entrada en vigor así que deberá estudiar los cambios normativos y comprender cómo van a afectar a sus operaciones. Tenga presente que el impacto del RGPD no se limita a un área específica de su actividad; exigirá adoptar un enfoque más orientado a los procesos en toda la empresa.

Es probable que deba modificar sus prácticas empresariales para cumplir con este nuevo reglamento y que tenga que establecer nuevos controles. Por tanto, ¿por dónde empezar? Hemos creado este sencillo gráfico para ayudarle a estructurar su enfoque de cumplimiento.



RGPD

- Entender los principales cambios que va a suponer esta legislación

Análisis rápido de la protección de datos

- Evaluar la actual arquitectura de datos, procesos y controles de riesgos y cumplimiento de su organización

Resultados y análisis de las auditorías

- Identificar los actuales riesgos
- Comprobar el grado de preparación de su empresa

Hoja de ruta de la implantación

- Desarrollar una hoja de ruta de la implantación que incorpore una arquitectura de cumplimiento
- Garantizar que el plan es realista y factible

Implantación

- Nombrar un asesor de confianza para:
  - identificar y documentar las actividades de procesamiento de datos
  - realizar evaluaciones de impacto de datos
  - desarrollar un plan de acción en respuesta a infracciones de datos
  - implantar procesos continuos de protección de datos
- Redactar una política detallada de protección de datos y definir un estándar que garantice que su empresa va a cumplir el RGPD
- Cuando sea necesario, nombrar a un Responsable de Protección de Datos y/o elegir un sistema de gestión de protección de datos para llevar a cabo un control continuo

Medición de la eficacia de la protección de datos

- Realizar un análisis de coincidencias y diferencias del RGPD o de la ISO 27001; se trata de evaluar la eficacia de sus esfuerzos en relación con el RGPD

Mejora continua

- Auditorías periódicas del RGPD y evaluaciones de impacto de la privacidad de los datos
- Asegurarse de que la gestión de riesgos de datos está integrada en la estructura global de gestión de riesgos
- Revisar periódicamente las necesidades de formación en la materia

Póngase en contacto con nosotros

Si quiere saber cómo podemos ayudar a su organización a comprender mejor los nuevos requisitos del RGPD para cumplir plenamente con este nuevo reglamento, póngase en contacto con uno de los siguientes especialistas.

Luis Pastor
Socio de Consultoría Tecnológica e Innovación
Luis.Pastor@es.gt.com

Víctor Gené
Asociado Senior (Legal / IT&IP)
Victor.Gene@es.gt.com

Grant Thornton
An instinct for growth™

grantthornton.es