

¿Está su empresa lista para el RGPD, la nueva legislación de protección de datos de Europa?

¿Qué es el RGPD?



El Reglamento General de Protección de Datos de la UE (RGPD)¹ revisa el marco legal relacionado con el manejo y procesamiento de datos personales de las empresas.

El RGPD entrará en vigencia el 25 de mayo de 2018. El objetivo de la RGPD (o GDPR por sus siglas en inglés) es establecer una mayor protección de los datos personales de los residentes de la UE al exigir que las empresas y las autoridades públicas cumplan con requisitos más estrictos. Estos requisitos se refieren a bases legales para el procesamiento de datos personales, los derechos de los interesados (por ejemplo, el “derecho de cancelación”), las transferencias transfronterizas de datos, la custodia de datos, las notificaciones de violación de datos y otros asuntos.

No tenemos filiales ni operaciones comerciales directas en Europa, ¿nos afecta RGPD?

Sí, el RGPD tiene un efecto global y puede aplicarse a cualquier empresa de América Latina que procese los datos personales de los residentes de la UE.

Un gran número de empresas sin operaciones directas en la UE todavía se ven afectadas por el RGPD.

Uno de los cambios más significativos resultantes del RGPD es la ampliación del alcance territorial del marco legal relevante. El RGPD prevé dos circunstancias en las que las organizaciones no establecidas en la UE estarían sujetas a sus disposiciones:

(1) Cuando los datos personales de los residentes de la UE están siendo procesados “por un controlador o un procesador no establecido en la Unión Europea” y “las actividades de procesamiento están relacionadas a ofrecer bienes o servicios a tales sujetos de datos, independientemente de si están conectados a un pago”²

(2) Cuando los datos personales de los residentes de la UE están siendo procesados “por un controlador o procesador no establecido en la Unión Europea y el “procesamiento se relaciona con el control del comportamiento de dichos sujetos de datos en la medida en que su comportamiento tenga lugar dentro de la UE”³.

Por lo tanto, el RGPD puede aplicarse a organizaciones de Centroamérica. Incluso cuando no participen en ninguna transacción comercial con entidades o consumidores de la UE.

Con base en las disposiciones adicionales del RGPD, en el caso del monitoreo, en particular, podría capturar un número de organizaciones con presencia en la web que se puede considerar que rastrean a una persona física “para tomar decisiones sobre él o para analizar o predecir sus preferencias personales, comportamientos y actitudes.”⁴ Organizaciones de fuera de la UE que entran

¹REGLAMENTO (EU) 2016/679. Del PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE Reglamento general de protección de datos

²Artículo 3 (2) (a) y Rec.23 RGPD

³Artículo 3 (2) (b) y Rec.24 RGPD

⁴Ibid.

en el RGPD están obligados a designar un representante (que actúe como punto de contacto) en la UE a menos que su procesamiento sea ocasional, no incluya datos confidenciales a gran escala y no sea probable que suponga un riesgo para los derechos de las personas.

¿Cuáles son las consecuencias del incumplimiento del RGPD?

Las consecuencias del incumplimiento son muy variadas. La multa máxima puede llegar a ser el cuatro por ciento de la facturación mundial anual o € 20 millones, lo que sea mayor.

La naturaleza, la gravedad y la duración de cualquier infracción o incumplimiento serán decisivos en la decisión de cualquier autoridad de supervisión que le corresponda imponer una multa. Las autoridades supervisoras también pueden exigir que las organizaciones que incumplan las normas tomen ciertas medidas correctivas, en lugar de multas o además de las mismas.

¿Cuáles son las principales disposiciones de RGPD?

- **Bases legales:** el procesamiento de datos debe basarse en una de las siguientes seis bases legales: consentimiento, interés legítimo primordial, cumplimiento del contrato, obligación legal, interés vital del interesado e interés público.
- **Principios de protección de datos:** las empresas deben poder demostrar el cumplimiento de los principios de minimización de datos, limitaciones de propósito y precisión.
- **Transparencia (deber de informar):** el RGPD aumenta la información que necesita incluir en sus avisos de privacidad. Deben ser concisos y legibles.
- **Derecho de los sujetos de datos:** los sujetos deben tener acceso a sus datos personales y la capacidad de exigir su eliminación y portabilidad. Todas las solicitudes deben cumplirse dentro de los 30 días. La política de gestión de solicitudes de una empresa debe introducirse con sus respuestas de plantilla.
- **Documentación:** las empresas deben conservar ciertos registros internos, pero ya no están obligadas a notificar a las autoridades de protección de datos sobre las actividades de protección de datos.

- **Relaciones laborales:** las empresas deben actualizar los contratos de trabajo y avisos a los empleados para que cumplan con el RGPD.
- **Externalización:** ciertas obligaciones estrictas deben estar contenidas en los contratos con los procesadores de datos (por ejemplo, auditoría obligatoria).
- **Transferencia de datos transfronteriza:** el RGPD prohíbe la transferencia de datos personales fuera de la UE a menos que se cumplan ciertas condiciones.
- **Procesos automatizados de toma de decisiones, incluidos los perfiles:** las personas deben tener derecho a optar por no participar.
- **Evaluación del impacto de la protección de datos:** se puede requerir cuando se lleva a cabo un procesamiento de "alto riesgo".
- **Notificación de violación de datos:** los datos deben mantenerse seguros y las violaciones de datos deben registrarse y notificarse a la autoridad supervisora (a menos que la violación no sea un riesgo para las personas) dentro de las 72 horas.
- **Seguridad / privacidad de datos por diseño, de forma predeterminada:** las empresas deben implementar medidas técnicas y organizativas adecuadas, tanto al momento de la determinación de los medios para el procesamiento como al momento del procesamiento. Cualquiera de estas medidas de privacidad por diseño puede incluir, por ejemplo, seudonimización u otras tecnologías que mejoran la privacidad.
- **Oficial de Gobernabilidad / Protección de Datos (DPO por sus siglas en inglés) / representante:** Dependiendo del procesamiento que lleve a cabo, es posible que necesite designar a un DPO. Los DPO no pueden ser despedidos ni penalizarse por desempeñar su función.

Para obtener más información, o si tiene alguna pregunta, envíe un correo electrónico a monserrat.guitart@dentons.com

SOBRE DENTONS

Dentons es la firma legal global más grande del mundo, comprometida a entregar siempre calidad y valor a sus clientes en todo el globo. Dentons es líder en el Índice Acritas 2016 Global Elite Brand, receptor del Premio BTI Client Service y ha sido reconocida por publicaciones de negocios y legales de primera línea en todo el mundo, gracias a sus innovaciones en servicio al cliente. Incluso, fundó Nextlaw Labs y la Nextlaw Global Referral Network. El enfoque policéntrico de Dentons, y su talento de talla mundial, retan el status quo para poder trabajar por los intereses de nuestros clientes en las comunidades en las que trabajamos y en las que vivimos.

dentons.com