

RGPD Folleto de cambios clave

El siguiente documento fue creado desde el sitio web: <https://euqdp.org/the-regulation/>.
Todo el texto fue tomado de este sitio web, no creado por asociación DIGIT.

El objetivo del RGPD es proteger a todos los ciudadanos de la UE de la privacidad y las violaciones de datos en el mundo actual basado en datos. Aunque los principios clave de la privacidad de los datos siguen siendo fieles a la directiva anterior, se han propuesto muchos cambios a las políticas regulatorias; Los puntos clave de RGPD, así como la información sobre los impactos que tendrá en las empresas, se pueden encontrar a continuación.



Mayor alcance territorial (aplicabilidad extraterritorial)

- Podría decirse que el cambio más grande en el panorama regulatorio de la privacidad de los datos viene con la **jurisdicción extendida del RGPD**, ya que se aplica a todas las compañías que procesan los datos personales de los interesados que residen en la Unión, independientemente de la ubicación de la campaña.
- Anteriormente, aplicabilidad territorial de la directiva era más ambigua.
- El RGPD también se aplica al procesamiento de datos personales de los interesados en la UE por un controlador o procesador no establecido en la UE (independientemente de si se requiere el pago) y el monitoreo de comportamiento que se produce dentro de la UE.

Penalizaciones

- Las organizaciones que infringen el RGPD pueden recibir una multa de **hasta el 4% de la facturación global anual o 20 millones de euros** (lo que sea mayor). Esta es la multa máxima que puede imponerse por las infracciones más graves, por ejemplo, no tener el suficiente consentimiento del cliente para procesar datos o violar el núcleo de los conceptos de Privacidad por Diseño.

Consentimiento

- Las **condiciones para el consentimiento se han fortalecido**, y las empresas ya no pueden usar términos y condiciones ilegibles largos llenos de información legal.
- La solicitud de consentimiento debe darse de forma inteligible y de fácil acceso, con el propósito de procesar la información a ese consentimiento.
- El consentimiento debe ser claro y distinguible de otros asuntos y debe proporcionarse de forma inteligible y de fácil acceso, utilizando un lenguaje claro y sencillo.
- Debe ser tan fácil retirar el consentimiento como darlo.

Notificación de incumplimiento

- Bajo el RGPD, las notificaciones de incumplimiento ahora son obligatorias en todos los estados miembros donde es probable que una violación de datos "genere un riesgo para los derechos y libertades de las personas".
- Esto debe hacerse dentro de las 72 horas posteriores a la primera toma de conciencia del incumplimiento. También se requiere que los procesadores de datos notifiquen a sus clientes, a los controladores, "sin demoras indebidas" después de darse cuenta por primera vez de una violación de datos.

Derecho de acceso

- Parte de los derechos ampliados de los interesados descritos por el RGPD es el derecho de los interesados a obtener una confirmación del controlador de datos sobre si se están procesando o no los datos personales que los conciernen, dónde y con qué fin.
- Además, el controlador debe proporcionar una copia de los datos personales, sin cargo, en formato electrónico. Este cambio es un cambio importante hacia la **transparencia de los datos** y el empoderamiento de los interesados.

Derecho al olvido

- También conocido como Borrado de datos, el derecho a ser olvidado da derecho al interesado a que el controlador de datos borre sus datos personales, deje de difundir más los datos y posiblemente haga que terceros detengan el procesamiento de los datos.

Portabilidad de datos

- El RGPD introduce la portabilidad de datos: el derecho de un sujeto interesado a recibir los datos personales que los conciernen.

Oficiales de Protección de Datos

- Bajo el RGPD no es necesario enviar notificaciones / registros a cada DPA local de actividades de procesamiento de datos, ni es un requisito para notificar / obtener aprobación para transferencias basadas en las Cláusulas de Contrato Modelo (CCMs).
- En cambio, existen **requisitos internos de mantenimiento de registro** como se explica más adelante, y la designación de OPD (Oficial de Protección de Datos) es obligatoria solo para aquellos cuyas actividades principales consisten en operaciones de procesamiento que requieren un monitoreo regular y sistemático de los **interesados a gran escala o categorías especiales de datos o datos relacionados con condenas penales y delitos**.
- Mayormente, el Oficial de Protección de Datos:
 - Debe ser nombrado sobre la base de las cualidades profesionales y, en particular, el conocimiento experto sobre legislación y las prácticas de protección de datos.
 - Puede ser un miembro del personal o un proveedor de servicios externo.
 - Los datos de contacto se deben proporcionar al DPA correspondiente.
 - Debe contar con los recursos adecuados para llevar a cabo sus tareas y mantener su conocimiento experto.
 - Debe informar directamente al más alto nivel de gestión.
 - No debe realizar ninguna otra tarea que pueda generar un conflicto de intereses.

Por favor considera las siguientes preguntas:

- 1. ¿Qué te parecen estas pautas? ¿Qué destaca en tu opinión?**
- 2. ¿Te ha afectado esto en tu vida personal o profesional? Si sí, ¿cómo?**
- 3. ¿Hay algo más que agregarías o cambiarías sobre las regulaciones del RGPD?**