Todo lo que tu empresa necesita saber sobre el RGPD

seresco *es soluciones*

seresco

RGPD 1

Todo lo que tu empresa necesita saber sobre el RGPD

1. Introducción

El 25 de mayo de 2018 comienza a aplicarse el nuevo Reglamento General de Protección de Datos. Este marco normativo europeo, que sustituye a la Ley Orgánica de Protección de Datos en España llevará a las organizaciones a adaptarse a los cambios que incorpora y cumplir así con sus obligaciones.

Aunque la ley entró en vigor en 2016, resulta frecuente encontrar empresas que todavía no tienen su sistema de gestión de la información completamente adecuado a la nueva normativa europea, bien por desconocimiento, bien por falta de tiempo o personal apropiado para llevarlo a cabo. A partir de la fecha en la que comienza a aplicarse el RGPD, esto es, el 25 de mayo, se verán sometidos a multas y sanciones si no aplican rigurosamente la norma.

Las implicaciones para el cumplimiento de RGPD son complejas, por lo que debemos estar al día de las novedades que supondrán para nuestra organización en todos los niveles: legal, administrativo y tecnológico.

2. Qué es el Reglamento General de Protección de Datos

El RGPD es la nueva normativa europea que en España sustituye a la Ley Orgánica de Protección de Datos.

El Reglamento General de Protección de Datos presenta varias características que lo hacen especialmente particular:

a. Su ámbito de aplicación territorial es inmenso pues abarca simultáneamente a los 28 países que forman la Unión Europea. Así, por primera vez, todas las empresas que operan en la UE participando en la obtención, procesamiento y uso de datos personales de los residentes en la UE están sometidas estrictamente a las condiciones exigidas por la nueva legislación. El RGPD afecta a relaciones B2B, B2C y a empresas ubicadas fuera del territorio de la Unión Europea pero que trabajan con datos de residentes dentro de la UE.

b. Cambia el modelo de protección de datos estipulado en la anterior normativa, es decir, en España la Ley Orgánica de Protección de Datos es sustituida por el Reglamento General de Protección de datos (GDPR). Se pasa a exigir la implantación de políticas activas de protección de datos dejando atrás las 'listas de comprobación' de la LOPD.

c. Se reconocen nuevos derechos a los titulares de los datos (derecho a la portabilidad, limitación del tratamiento, derecho a la supresión -derecho al olvido-). Así, por ejemplo, por el derecho a la portabilidad, los ciudadanos

tienen derecho a recibir una copia de sus datos a través de la organización de los que procedan.

d. Se crea una nueva figura: el Delegado de Protección de Datos (DPO). Será el encargado de asesorar y supervisar al responsable sobre las políticas de protección de datos de las empresas. Este nuevo cargo exigirá cualificación en materia jurídica, técnica y empresarial. La función del DPO se puede llevar a cabo interna o externamente a la organización. Aunque no es obligatorio para todas las empresas, es una figura más que recomendable a tener en cuenta, pues, tal como indica la Agencia Española de Protección de Datos, 'constituye uno de los elementos claves del RGPD y un garante del cumplimiento de la normativa de protección de datos en las organizaciones'.

e. Se presta atención especial a la ciberseguridad. La empresa está obligada a notificar las violaciones de seguridad de los datos personales que sufran, estableciendo un plazo máximo de 72h desde que las detecta hasta que las denuncia a la autoridad de control competente. El RGPD (art.82) reconoce el derecho a toda persona que sufra daños o perjuicios materiales o morales como consecuencia de una infracción de la norma a solicitar una indemnización al responsable o encargado del tratamiento. Una empresa que sea ciberatacada, por tanto, puede sufrir consecuencias administrativas (sanción) y civiles (indemnización), si no se toman las medidas de responsabilidad activa pertinentes. Así mismo, siempre es obligatorio es comunicar las brechas de seguridad.

En definitiva, el objetivo principal de la RGPD se centra en proteger el Derecho Fundamental a la Privacidad de todas las personas de la UE, especialmente en un contexto tan sensible como el que nos encontramos en plena transformación digital con la continua exposición de datos de los ciudadanos.

Desde el 25 de mayo de 2018 toda empresa de la Unión Europea o que opere con datos de ciudadanos de la UE se encuentra en la obligación de conocer:

1. **Qué información recopila**
2. **Cuándo se recopila la información**
3. **En dónde se almacena la información**

Las organizaciones tienen que garantizar la privacidad de todas las personas físicas y dejar bien claro cómo lo van a hacer, pudiendo demostrar en todo momento que han obtenido consentimiento de la persona tratada para guardar sus datos, que han explicitado cómo van a proteger dichos datos y que han registrado también cuál será la finalidad de su uso.

3. Cómo va a afectar a tu empresa el RGPD

Todas las organizaciones dentro de la Unión Europea y que operen con ciudadanos de la UE están sujetas al control del Reglamento General de Protección de Datos.

Tu empresa va a tener que someterse a cambios, seguro. De lo contrario se verá expuesta a elevadas sanciones, cuantiosas multas y problemas de reputación. En concreto, la sanción puede alcanzar hasta 20 millones de euros o el 4% de la facturación de la compañía, la cantidad que sea mayor.

El RGPD, en su artículo 35, expone que, en aquellos tratamientos que puedan comportar un

riesgo significativo (alto) para los derechos y las libertades de las personas físicas es obligatorio hacer la denominada Evaluación de Impacto de Protección de Datos (PIA siglas en inglés). Consiste en un procedimiento que revisa los riesgos de privacidad derivados de la obtención y tratamiento de datos personales antes de que se lleven a cabo en la organización. Así se pueden tomar medidas preventivas para evitar o atenuar los posibles riesgos detectados.

Básicamente, hay que determinar la probabilidad de que se produzcan situaciones no deseadas y su gravedad. No es necesaria la redacción de una Evaluación de Impacto de Protección de Datos en todos los casos, aunque es recomendable.
Las empresas obligadas a realizar la Evaluación de Impacto de Protección de Datos son aquellas que manejan volúmenes de datos especialmente sensibles, como por ejemplo:

- **Farmacéuticas**
- **Hospitales, clínicas, centros de salud**
- **Seguridad privada y vigilancia**
- **Colegios, escuelas, universidades**
- **Empresas comercializadoras de energía**
- **Empresas que realicen e-commerce**
- **...**

En definitiva, todas aquellas organizaciones que gestionen un tratamiento de datos que vayan a entrañar un alto riesgo para los derechos y libertades de las personas físicas tienen que llevar a cabo la Evaluación de Impacto de Protección de Datos.

Si esta evaluación diagnostica la presencia de riesgo elevado para los derechos o libertades de los implicados y no se toman medidas, habrá que consultar a la Asociación Española de Protección de Datos antes de comenzar el tratamiento de esa información. Será la AEPD la que revisará la evaluación y tome la decisión de recomendar acciones a tomar, solicitar más información o, incluso, prohibir a la empresa el tratamiento de los datos.

4. Qué medidas tiene que tomar tu empresa

El 25 de mayo de 2018 se hace efectivo el RGPD, por lo que su cumplimiento es obligatorio desde esa fecha. Las multas que puede imponer la AEPD ascenderán a cantidades altísimas, especialmente en casos de no notificación de fugas de datos por ciberataques a la autoridad competente. Existen dos categorías de sanciones que pueden llegar a los 20 millones de euros o el 4% de la facturación global de la compañía.

Las organizaciones deben revisar sus actuales sistemas de tratamiento de información para garantizar la privacidad de los ciudadanos y deberán hacerlo desde diferentes puntos de vista:

1. **Sus procesos administrativos se adecúan al nuevo marco normativo**
2. **Su contexto legislativo obedece las condiciones del nuevo reglamento**
3. **Sus sistemas informáticos permiten un tratamiento de la información seguro y controlado**

Los datos personales en una organización ya no se procesarán sin permiso voluntario y directo del interesado y tendrán que:

- Procesarse de manera adecuada a la normativa del RGPD y con un fin definido para el que se solicitan exclusivamente.
- Deben ser correctos, actualizados y tienen que estar asegurados informáticamente.
- En caso de que ya no se necesiten para el propósito con el que fueron solicitados deben eliminarse.

5. Conclusiones

El Reglamento General de Protección de Datos (RGPD) es aplicable a partir del 25 de mayo de 2018. Desde esa fecha todas las empresas que operen en la Unión Europea o con datos de ciudadanos residentes en la UE deben someterse a su cumplimiento bajo riesgo de importantes sanciones y multas en caso de no hacerlo (pueden producirse sanciones de hasta 20 millones de euros o el 4% de la facturación global de la compañía).

Además, determinadas empresas deberán nombrar a un Delegado de Protección de Datos (DPO), bien de forma interna, bien de forma externa, para que sea el responsable de diseñar los mecanismos internos de cumplimiento de RGPD, realizar el inventario de tratamiento de datos y monitorizar estrictamente su cumplimiento.

En caso de organizaciones con un tratamiento de información protegida por ley y más sensible para las personas físicas (religión, raza, salud, antecedentes penales...), se aplicará obligatoriamente una Evaluación de Impacto de Protección de Datos para detectar de antemano posibles riesgos.

La ciberseguridad adquiere un papel protagonista: si una empresa es ciberatacada debe notificarlo en menos de 72h a la autoridad de control pertinente. En España, la Agencia Española de Protección de Datos (AEPD). El no hacerlo podrá acarrear consecuencias tanto por vía administrativa (sanciones de hasta 600.000 por la AEPD) como por vía civil (art. 82 RGPD).

Aunque en España ya contábamos con una Ley Orgánica de Protección de Datos bastante estricta en términos de tratamiento de información, el nuevo Reglamento General de Protección de Datos europeo supondrá la obligación de revisar y modificar procedimientos en todas las organizaciones.

www.seresco.es
www.masquenomina.es
soluciones@seresco.es
902 01 34 64

seresco *es soluciones*

seresco