

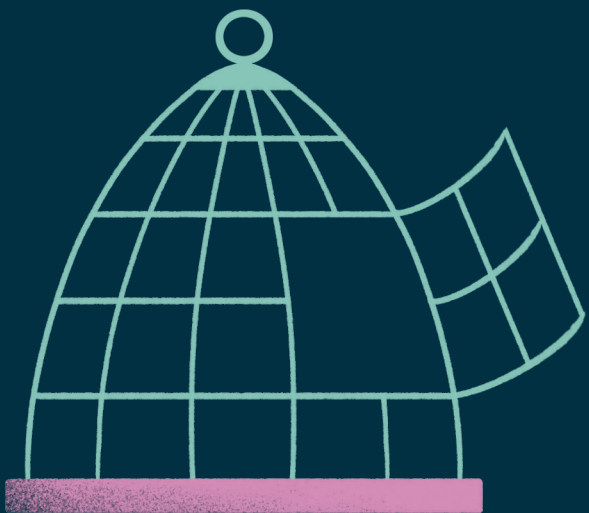


RGPD

En esta era digital, los datos personales son oro puro. Su buen uso y resguardo se ha convertido en una prioridad de los consumidores, que valoran enormemente su privacidad. Para mejorar su cuidado y tratamiento, hace justo un año la Unión Europea puso en marcha el nuevo Reglamento General de Protección de Datos (RGPD), que ha generado una revolución en la manera en que las compañías tratan la información de sus usuarios. ¿Su empresa ya está al día?

¿GUARDA DATOS DE SUS CLIENTES?

ASEGÚRESE DE QUE LO HACE BIEN



01.

¿QUÉ ES EL RGPD?

El Reglamento General de Protección de Datos (RGPD) es una serie de requisitos mínimos que las compañías, sin importar su tamaño, deben cumplir con respecto al cuidado de la información de sus clientes.

Su objetivo es que las empresas protejan los datos de sus usuarios con la mayor diligencia, siendo además transparentes sobre a qué harán con ellos, quién es el responsable de su manejo, cómo se han obtenido, cuánto tiempo los tendrán y si serán cedidos a terceros, por ejemplo.



¿APLICA A TODAS LAS EMPRESAS?

El reglamento aplica a grandes, medianas y pequeñas compañías, incluso a los autónomos, siempre y cuando usen datos personales como parte de sus actividades dentro de la UE. Pero si el tratamiento de datos no constituye la parte principal de sus negocios, no están sujetas a algunas obligaciones. Por

ejemplo, las pymes solo deben llevar un registro si el manejo es regular. "Para la mayoría de las grandes empresas es casi obligatorio. Muchas de ellas ya se han puesto al día", comenta Elisabet Iglesias, responsable de Seguridad para Transformación Digital en Telefónica Empresas".

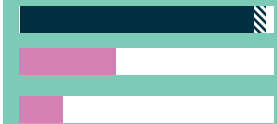
¿QUÉ DATOS SE PUEDEN TRATAR?

Nombre y apellidos, domicilio, dirección de correo electrónico, número del documento de identidad, datos de la dirección IP y el identificador de una *cookie*. El reglamento prohíbe el tratamiento de datos sensibles como el origen étnico, racial, la opción política, religiosa o sindical. También los relativos a la salud (en caso

de que el negocio no esté vinculado a este sector), a la orientación sexual y los datos biométricos y genéticos. "Hay que considerar todo esto al prestar un servicio o al contratar a un proveedor", dice Gustavo San Felipe, Delegado de Protección de Datos de Acens, una compañía de Telefónica Empresas.

¡OJO AL DATO!

• Entre el **92%** y **97%** de las pymes españolas maneja datos de clientes, proveedores y empleados. Y en menor medida controla datos relativos a videovigilancia (**38%**) y formularios en Internet (**17%**). Cepyyme



• Más del **90%** de los europeos quiere tener el mismo derecho a la protección de sus datos en toda la UE, con independencia del país en el que se procesen. CE



• Solo el **18%** de los ciudadanos cree que tiene un control absoluto sobre la información que facilita por internet. CE



02.

OCHO PREMISAS CLAVE QUE DEBE CUMPLIR SU EMPRESA

1

SEA TRANSPARENTE

- Preséntese ante sus usuarios cuando solicite datos.
- Diga por qué tratará la información y durante cuánto tiempo la guardará.
- Use un lenguaje sencillo.



2

SOLICITE SU USO

El consentimiento sobre el uso de datos debe darse mediante una acción afirmativa clara.

3

FACILITE EL ACCESO

Las empresas deben facilitar que las personas accedan a sus datos para ejercer sus derechos de rectificación o cancelación.

4

CUMPLA EL DERECHO AL OLVIDO

Los datos deben ser borrados cuando la función para la cual fueron recogidos haya dejado de existir.

5

OFREZCA OPCIONES

Permita que las personas opten a no recibir la publicidad directa que utiliza sus datos. Recuerde, la nueva regulación prohíbe las comunicaciones electrónicas no solicitadas por cualquier medio, como correos electrónicos, mensajes de texto e incluso algunas llamadas telefónicas, si los usuarios no han dado su consentimiento.

6

¿RECOPILA DATOS DE MENORES DE 16 AÑOS?

Según el reglamento debe obtener el consentimiento paterno. Sin embargo, cada Estado miembro de la Unión Europea puede reducir este límite a entre 13 y 16 años. Por tanto, verifique el límite de edad.



7

PROTEJA

Si conserva los datos en un sistema informático, restrinja el acceso a los archivos o actualice periódicamente la configuración de sus sistemas de seguridad.

8

PIDA GARANTÍAS

Si los datos están en la nube, asegúrese de que su proveedor cumple la regulación. "Seremos responsables de lo que ocurra con ellos. Es imprescindible que el operador *cloud* garantice su seguridad. Acens es hoy una de las mejores opciones en el mercado", dice Tomás F. Serna, abogado independiente experto en protección de datos.

"Se trata de que las organizaciones sean transparentes sobre los datos que manejan": Gustavo San Felipe, DPO en Acens.



03.

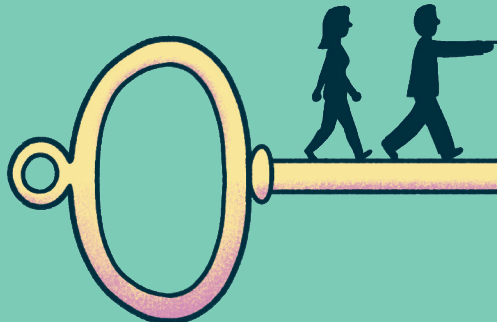
¿YA HA ELEGIDO DELEGADO?

Con la finalidad de que las empresas cuiden de manera constante la información de sus clientes, las autoridades de la UE han establecido la figura del delegado de protección de datos o DPO, del inglés *Data Protection Officer*. “Se trata del velador del reglamento”, afirma San Felipe.



¿CUÁLES SON SUS FUNCIONES?

Informar y asesorar a los responsables y encargados del tratamiento de los datos personales sobre las obligaciones que tienen. Supervisan el cumplimiento de la legislación. “Las grandes empresas forman a su personal para tener esta figura, pero el perfil es complejo: navega entre el mundo tecnológico y el jurídico”, dice Iglesias.



¿MI EMPRESA LO NECESITA?

No todas las empresas están obligadas a tener un delegado. Aquellas compañías (casi siempre pymes) cuyo tratamiento de datos no implique la parte principal de su negocio no están sujetas a esta figura. “Pero siempre es recomendable contar con un delegado: da certeza, seguridad y confianza de cara al público. Demuestra el compromiso con el reglamento y con los principios básicos que defiende”, asegura el DPO de Acens. En este sentido, la posibilidad de subcontratar el servicio de DPO es una opción muy a tener en cuenta especialmente para las pymes.

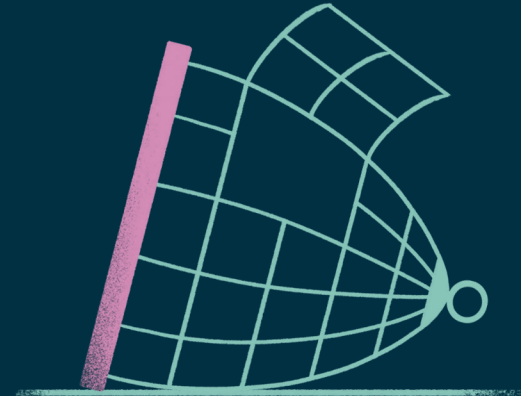
04.

SANCIONES

El coste de incumplir la normativa puede ser elevado y va desde:

- Una amonestación.
- La suspensión del tratamiento de datos.
- Una multa de hasta 20 millones de euros o del 4% del volumen de negocio anual de la compañía.

Elisabet Iglesias, responsable de Seguridad para Transformación Digital en Telefónica Empresas: “Hay que considerar el daño reputacional. Las sanciones son públicas y eso afecta a la imagen”.



¿Quién es la autoridad de protección de datos?

La Agencia Española de Protección de Datos (además de las Agencias Vasca y Catalana) y el Comité Europeo de Protección de Datos.