Comisión Europea

Siete pasos para que las empresas

se preparen para el Reglamento general de protección de datos (RGPD)

Justicia y Consumidores

¿A quién va dirigida?

Esta guía tiene por objeto ayudar a las empresas que no manejan datos personales como actividad principal, como las pymes que tratan principalmente los datos personales de sus empleados o que disponen de listas de sus clientes y consumidores. Dichas empresas incluyen, por ejemplo, comerciantes y tiendas, como una panadería o una carnicería, o proveedores de servicios, como los arquitectos. Esta guía destaca los pocos pasos que deben seguir para prepararse para el RGPD.

Los datos personales son toda información relativa a una persona física viva identificada o identificable (no las personas jurídicas), e incluyen, por ejemplo: el nombre, los apellidos, el domicilio, la dirección de correo electrónico o los datos de localización del mapa de su móvil. Este suele ser el caso de los datos que usted pueda tener sobre sus empleados, clientes o proveedores.

Cuanto menos riesgo supongan sus actividades para los datos personales, menos deberá hacer.

Aplique principios clave:

- **recopile los datos personales para un fin claramente definido y no los use para otros propósitos** (si pide a sus clientes que le faciliten el correo electrónico para poder recibir sus nuevas ofertas o promociones, no puede utilizarlo para nada más ni venderlo a otras empresas).
- **no recopile más datos de los que necesite** (si hace entregas a domicilio, necesitará, por ejemplo, una dirección y un nombre del portero automático, pero no necesitará saber si su cliente es soltero o está casado); simplemente tenga en cuenta los datos personales que tiene bajo su control.

PASO 1 VERIFIQUE LOS DATOS PERSONALES QUE RECOPILA Y TRATA, EL FIN PARA EL QUE LO HACE Y SOBRE QUÉ BASE JURÍDICA

Usted tiene **empleados**; trata sus datos personales basándose en el contrato de trabajo y en las obligaciones legales (como las de informar a las autoridades tributarias o al sistema de la Seguridad Social).

Puede gestionar una lista de **clientes particulares**, por ejemplo, para enviarles información sobre ofertas especiales o anuncios si obtuvo el consentimiento de dichos clientes.

No siempre necesitará el consentimiento. Existen casos en los que las personas esperarán que trate sus datos personales. Por ejemplo, como vendedor de pizzas, puede usar la dirección de entrega para anunciar uno de sus nuevos productos. Esto se denomina interés legítimo. Debe informar a las personas sobre el uso que pretende hacer de los datos y dejar de tratarlos si así se lo piden.

Si gestiona una lista de **proveedores** o **clientes comerciales**, hágalo basándose en los contratos que tenga con ellos. Estos contratos no tienen que ser por escrito.

PASO 2 INFORME A SUS CLIENTES, EMPLEADOS Y OTRAS PERSONAS CUANDO RECOPILE SUS DATOS PERSONALES

Las personas deben saber que usted está tratando sus datos personales y conocer el fin para el que lo hace.

Sin embargo, no tiene que advertirles cuando ya dispongan de información sobre cómo utilizará sus datos, por ejemplo, cuando un cliente le pide que haga una entrega a domicilio.

Asimismo, debe informar a las personas sobre los datos personales que posee sobre ellas y permitirles acceder a dichos datos si así se lo solicitan. Conserve los datos ordenados, de forma que pueda responder fácilmente y sin problemas si, por ejemplo, un empleado le solicita información sobre el tipo de datos personales que usted guarda.

PASO 3 CONSERVE LOS DATOS PERSONALES ÚNICAMENTE MIENTRAS SEA NECESARIO

Datos sobre sus empleados: mientras dure la relación laboral y las obligaciones legales correspondientes.

Datos sobre sus clientes: mientras dure la relación con el cliente y las obligaciones legales correspondientes (por ejemplo, a efectos fiscales).

Borre los datos cuando ya no sean necesarios para el fin para el que fueron recopilados.

PASO 4 PROTEJA LOS DATOS PERSONALES QUE ESTÉ TRATANDO

Si conserva estos datos en un **sistema informático**, restrinja el acceso a los archivos que contienen los datos, por ejemplo, con una contraseña, y actualice periódicamente la configuración de seguridad de su sistema.

(Nota: el RGPD no recomienda el uso de ningún sistema informático específico).

Si conserva documentos físicos con datos personales, asegúrese de que no sean accesibles a personas sin autorización; ciérrelos con llave en una caja fuerte o armario seguro.

PASO 5 CONSERVE DOCUMENTACIÓN SOBRE SUS ACTIVIDADES DE TRATAMIENTO DE DATOS

Prepare un documento breve que explique qué datos personales conserva y con qué motivos. Puede que se le exija poner esta documentación a disposición de su autoridad nacional de protección de datos si así se lo solicita.

Esta documentación debería incluir la información siguiente.

INFORMACIÓN	EJEMPLOS
Finalidad del tratamiento de los datos	Avisar a los clientes de ofertas especiales/prestar servicios de entrega a domicilio; pagar a los proveedores; sueldos y cobertura de la Seguridad Social para los empleados.
Tipos de datos personales	Información de contacto de los clientes; información de contacto de los proveedores; datos de los empleados.
Categorías de personas concernidas	Empleados; clientes; proveedores.
Categorías de destinatarios	Autoridades laborales; autoridades fiscales.
Períodos de conservación	Los datos personales de los empleados, hasta el término del contrato (y de las obligaciones legales asociadas); los datos personales de los clientes, hasta el final de la relación con el cliente o del contrato.
Medidas técnicas y organizativas para proteger los datos personales	Soluciones de seguridad informática actualizadas periódicamente; armario cerrado con llave/caja fuerte.
Si los datos personales se transfieren a destinatarios fuera de la UE	Uso de un sistema de procesamiento de información fuera de la UE (por ejemplo, almacenamiento en la nube).

PASO 6 ASEGÚRESE DE QUE SU SUBCONTRATISTA RESPETA LAS NORMAS

Si subcontrata el tratamiento de los datos personales a otra empresa, utilice únicamente un proveedor de servicios que garantice el cumplimiento de los requisitos del RGPD (por ejemplo, las medidas de seguridad). Antes de firmar un contrato, compruebe si la empresa seleccionada ha realizado los cambios necesarios y se ha adaptado al RGPD. Inclúyalo en el contrato.

PASO 7 COMPRUEBE SI ESTÁ SUJETO A LAS SIGUIENTES DISPOSICIONES

> Para proteger mejor los datos personales, las empresas pueden tener que nombrar un Delegado de Protección de Datos (DPD). **Sin embargo, no tiene que nombrar un Delegado de Protección de Datos** si el tratamiento de datos personales no constituye la parte principal de su negocio, no es un tratamiento de alto riesgo y su actividad no se realiza a gran escala.

Por ejemplo, si su negocio únicamente recaba datos sobre sus clientes para realizar entregas a domicilio, no deberá nombrar un DPD.

Incluso si debe contar con un DPD, esta persona podría ser un empleado existente al que se encomendara esta función además de otras tareas. O podría ser un consultor externo; del mismo modo que muchas empresas utilizan contables externos.

> **Normalmente, no deberá llevar a cabo ninguna evaluación de impacto relativa a la protección de datos.**

La evaluación de impacto se reserva para aquellas empresas cuyo tratamiento supone un mayor riesgo para los datos personales; por ejemplo, si realizan un seguimiento a gran escala de una zona de acceso público (como la videovigilancia).

Si su empresa es una pyme que gestiona los salarios de los empleados y una lista de clientes, no necesita llevar a cabo ninguna evaluación de impacto de estas operaciones de tratamiento.

Multas

Las autoridades de protección de datos están facultadas para sancionar las infracciones de las normas de protección de datos. Pueden adoptar medidas correctivas (tales como una orden o la suspensión temporal del tratamiento) o imponer multas.

Su decisión de imponer una multa debe ser proporcional y basarse en una evaluación de todas las circunstancias de cada caso individual.

Si deciden imponer una multa, su importe dependerá también de las circunstancias particulares del caso, tales como la gravedad de la infracción o si la infracción fue intencionada o por negligencia. Además, tendrán en cuenta su actitud y sus intenciones.

Si desea obtener más información:

1. **Visite la guía en línea de la Comisión Europea sobre la reforma de la protección de datos (disponible en todas las lenguas de la UE):**

   europa.eu/dataprotection/es

2. **Consulte a su autoridad nacional de protección de datos:**

   edpb.europa.eu/es

AVISO IMPORTANTE

La información de esta guía tiene el objetivo de contribuir a comprender mejor las normas de protección de datos de la UE.

Tiene un carácter meramente orientativo; solo el texto del Reglamento general de protección de datos (RGPD) tiene validez legal. Por consiguiente, solo el RGPD puede generar derechos y obligaciones para las personas. Esta orientación no crea ningún derecho efectivo o expectativa.

La interpretación vinculante de la legislación de la UE es una competencia exclusiva del Tribunal de Justicia de la Unión Europea. Las opiniones expresadas en esta orientación deben entenderse sin perjuicio de la posición que pueda adoptar la Comisión ante el Tribunal de Justicia.

Ni la Comisión Europea ni ninguna otra persona que actúe en su nombre son responsables del uso que pueda hacerse de la información de esta guía.

Dado que este documento refleja el estado en el momento de su elaboración, deberá considerarse como una «herramienta viva» abierta a mejoras y su contenido puede estar sujeto a modificaciones sin previo aviso.

Oficina de Publicaciones de la Unión Europea

Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2019

Print	PDF
ISBN 978-92-76-03579-4	ISBN 978-92-76-03595-4
doi:10.2838/345293	doi:10.2838/656137
DS-02-19-307-ES-C	DS-02-19-307-ES-N