



RGPD: nuevas oportunidades, nuevas obligaciones



Lo que las **empresas** tienen que saber
sobre el Reglamento general de protección
de datos de la Unión Europea

Printed by Bietlot in Belgium

Ni la Comisión Europea ni nadie que actúe en su nombre se responsabilizarán del uso que pudiera hacerse de esta información.

Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2018

© Unión Europea, 2018

Reutilización autorizada, con indicación de la fuente bibliográfica.

La política relativa a la reutilización de los documentos de la Comisión Europea fue establecida por la Decisión 2011/833/UE (DO L 330 de 14.12.2011, p. 39).

Print	ISBN 978-92-79-79446-9	doi:10.2838/14169	DS-01-18-082-ES-C
PDF	ISBN 978-92-79-79431-5	doi:10.2838/351308	DS-01-18-082-ES-N

ÍNDICE

CAPÍTULO 1

UNA OPORTUNIDAD DE NEGOCIO..... 2

CAPÍTULO 2

COMPRENSIÓN DEL RGPD..... 4

CAPÍTULO 3

SUS OBLIGACIONES SEGÚN EL RGPD..... 8

CAPÍTULO 4

¿PREPARADO PARA CUMPLIRLO?..... 18



CAPÍTULO 1

UNA OPORTUNIDAD DE NEGOCIO

El Reglamento general de protección de datos (RGPD) de la Unión Europea (UE) regula la forma en que las empresas tratan y gestionan los datos personales. Con efecto a partir del 25 de mayo de 2018 y de aplicación a todas las empresas y organizaciones (como hospitales, administraciones públicas, etc.), constituye el mayor cambio en las normas de protección de datos de la Unión en más de veinte años.

El RGPD no solo confiere más control a los ciudadanos sobre cómo se usan sus datos personales, sino que

también simplifica considerablemente el marco normativo para las empresas. Con este fin, establece un marco uniforme para la legislación en materia de protección de datos en toda la UE. En otras palabras, en lugar de que cada país cuente con su propia legislación sobre protección de datos, ahora toda la UE se rige por un único reglamento. Por tanto, una empresa que opere en diferentes países ya no necesita cumplir varias —a menudo distintas— normativas y solo tiene que ajustarse a los requisitos del RGPD para ofrecer sus servicios en cualquier lugar de la UE.

¿Cómo puede beneficiar el RGPD a su empresa?

- 👤 **Una Unión, una legislación:** una única normativa hace que sea más sencillo y barato para las empresas hacer negocios en la UE.
- 👤 **Ventanilla única:** en la mayoría de los casos, las empresas únicamente tienen que tratar con una autoridad de protección de datos (APD).
- 👤 **Normas europeas en suelo europeo:** las empresas de fuera de la UE deben aplicar las mismas normas que las empresas europeas al ofrecer sus bienes y servicios a ciudadanos de la UE.
- 👤 **Enfoque basado en los riesgos:** el RGPD evita establecer una obligación onerosa y universalmente aplicable y, en lugar de esto, adapta las obligaciones a los riesgos respectivos.
- 👤 **Las normas se adecuan a la innovación:** el RGPD es tecnológicamente neutro.

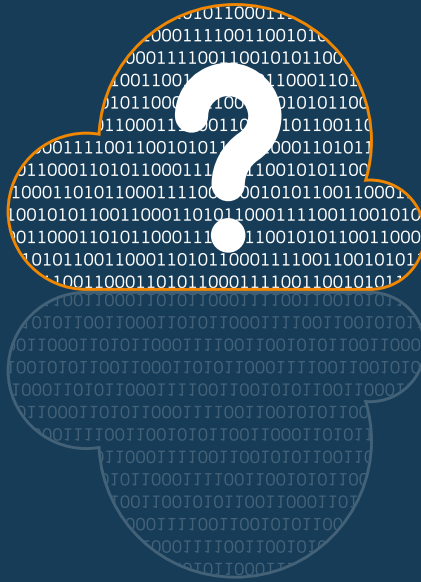
Todo se trata de confianza

La protección de datos personales es una preocupación importante para las personas. Por tanto, su confianza en los entornos digitales sigue siendo baja. Según una encuesta del Eurobarómetro:

- 👤 ocho de cada diez personas creen que no tienen pleno control de sus datos personales,
- 👤 seis de cada diez no confían en los negocios en línea,
- 👤 más del 90 % de los europeos afirman que quieren los mismos derechos de protección de datos en todos los países de la UE.

El RGPD representa una nueva oportunidad para que su negocio mejore la confianza de los consumidores mediante la gestión de los datos personales basada en los riesgos.

«Las empresas que no protegen adecuadamente los datos personales de las personas se arriesgan a perder la confianza de los consumidores, la cual es fundamental para animarles a utilizar nuevos productos y servicios.»



CAPÍTULO 2

COMPRENSIÓN DEL RGPD

¿Debo cumplir el RGPD?

En resumen, el RGPD se aplica a **cualquier** empresa que **trate datos personales** mediante el tratamiento **automatizado** o **manual** (siempre que los datos se organicen con arreglo a criterios).

Incluso si su empresa únicamente trata datos por cuenta de otras empresas, seguirá teniendo que cumplir las normas.

El RGPD se aplica en los casos siguientes:

- 📍 su empresa trata datos personales y tiene sede en la UE, independientemente de dónde tenga lugar el tratamiento de datos, o
- 📍 su empresa está establecida fuera de la UE, pero ofrece productos o servicios a personas dentro de la UE u observa el comportamiento de estas.

¿Qué son los datos personales?

Los datos personales se refieren a toda la información relativa a una persona física viva identificada o identificable y pueden incluir lo siguiente:

- 📍 el nombre,
- 📍 la dirección y el número de teléfono,
- 📍 la ubicación,
- 📍 los registros sanitarios,
- 📍 los ingresos y la información bancaria,
- 📍 las preferencias culturales,
- 📍 ... y más.

Los datos personales que hayan sido desidentificados o seudonimizados, pero que todavía puedan utilizarse

para volver a identificar a una persona, también se inscriben en el ámbito de aplicación del RGPD. Sin embargo, los datos personales que hayan sido convertidos irreversiblemente en anónimos, de forma que la persona deje de ser identificable, no se consideran datos personales y, por tanto, no se rigen por el RGPD.

El RGPD también es tecnológicamente neutro, lo que significa que protege los datos personales independientemente de la tecnología utilizada o de cómo se conserven los datos personales. Con independencia de si su empresa trata y conserva datos personales utilizando un sistema informático complejo o a través de archivos en papel, usted estará sujeto al RGPD.

«Con independencia de si su empresa trata y conserva datos personales utilizando un sistema informático complejo o a través de archivos en papel, usted estará sujeto al RGPD».

Sea extremadamente cuidadoso con las categorías especiales (sensibles) de datos personales

Si los datos personales que recoge incluyen información sobre la salud, la raza, la orientación sexual, la religión, las creencias políticas o la afiliación sindical, se consideran datos sensibles. Su empresa únicamente puede tratar estos datos en determinadas condiciones y puede que tenga que implantar garantías adicionales, como el cifrado.

¿Qué constituye tratamiento de datos personales?

Según el RGPD, las acciones como la recogida, la utilización y la supresión de datos personales están incluidas en la definición de tratamiento de datos personales.

¿Controla sus instalaciones a través de un circuito cerrado de televisión? ¿Consulta una base de datos que contiene datos personales con fines empresariales? ¿Envía correos

electrónicos promocionales? ¿Borra archivos (digitales) de empleados o destruye documentos? ¿Publica una foto de una persona en su sitio web o canales de medios sociales?

Si su respuesta a cualquiera de las preguntas anteriores es «sí», sin duda su empresa trata datos personales.

¿Cómo ayuda el RGPD a reducir costes?

El RGPD tiene en cuenta las necesidades de las empresas. Por ejemplo, el Reglamento tiene como objetivo eliminar los requisitos administrativos a fin de reducir los costes y minimizar las cargas administrativas:

- 📌 **No más notificaciones previas:** la reforma elimina la mayoría de las notificaciones previas a las autoridades de control, junto con sus costes asociados.
- 📌 **Delegados de protección de datos (DPD):** principalmente las empresas tienen que nombrar un DPD si sus actividades principales implican el tratamiento de datos sensibles a gran escala o la observación a gran escala, habitual y sistemática de personas; las administraciones públicas tienen la obligación de nombrar un DPD.

- 📌 **Evaluaciones de impacto relativas a la protección de datos:** las empresas únicamente están obligadas a llevar a cabo una evaluación de impacto relativa a la protección de datos si una actividad de tratamiento de datos propuesta entraña un alto riesgo para los derechos y libertades de las personas.
- 📌 **Conservación de registros:** las empresas con menos de 250 empleados no deben llevar registros, a menos que el tratamiento de datos no sea accidental o implique información sensible.

«El Reglamento tiene como objetivo eliminar los requisitos administrativos a fin de reducir los costes y minimizar las cargas administrativas».



CAPÍTULO 3

SUS OBLIGACIONES SEGÚN EL RGPD

El RGPD impone a las empresas obligaciones directas en materia de tratamiento de datos a escala de la UE. Según el RGPD, una empresa *solo* puede tratar datos personales en determinadas condiciones. Por ejemplo, el tratamiento debe ser justo y transparente, tener un fin especificado y legítimo y limitarse a los datos necesarios para cumplir dicho fin. Asimismo, debe basarse en uno de los siguientes fundamentos jurídicos.

- 👤 El **consentimiento** de la persona de que se trate.
- 👤 Una **obligación contractual** entre usted y el interesado.
- 👤 El cumplimiento de una **obligación legal**.
- 👤 La protección de los **intereses vitales** del interesado.
- 👤 La realización de una **misión en interés público**.
- 👤 La satisfacción de los **intereses legítimos** de su empresa, pero solo tras haber comprobado que los derechos y libertades fundamentales de la persona cuyos datos estén tratando no se vean afectados significativamente. Si los derechos de la persona prevalecen sobre sus intereses, usted no podrá tratar los datos.

En el punto de mira: obtener el consentimiento para el uso de datos personales

El RGPD aplica normas estrictas para el tratamiento de datos basado en el consentimiento. El objetivo de estas normas es garantizar que la persona entienda a qué está dando su consentimiento. Esto significa que el consentimiento debe **darse libremente y ser específico, informado e inequívoco** mediante una solicitud presentada en un lenguaje claro y sencillo. Además, el consentimiento debe darse mediante un **acto afirmativo**, como el marcado de una casilla en línea o la firma de un formulario.

Si usted trata datos personales de **menores** basándose en el consentimiento, es necesario el consentimiento parental. Sin embargo, como el límite de edad varía entre los 13 y los 16 años según los países, se aconseja consultar la legislación nacional.

*¡Recuerde!
Cuando alguien
consiente el tratamiento
de sus datos personales,
usted solo podrá tratarlos
para los fines para los que se haya
dado el consentimiento. Además,
debe darle la oportunidad de retirar
su consentimiento.*

Definición de su función y responsabilidad

Una vez que haya determinado que el RGPD se aplica a su empresa y que existe tratamiento de datos personales, el siguiente paso es la definición de su función.

Las normas de protección de datos distinguen entre el responsable del tratamiento y el encargado del tratamiento, cada uno con diferentes obligaciones. Mientras que el responsable del tratamiento determina el fin y los medios del tratamiento de los datos personales, el encargado del tratamiento trata únicamente los datos personales por cuenta del responsable del tratamiento. No obstante, esto no significa que el encargado simplemente pueda esconderse detrás del responsable del tratamiento.

EL RGPD exige que un responsable del tratamiento recurra únicamente a un encargado del tratamiento que ofrezca garantías suficientes, que deben estar incluidas en un contrato escrito entre el responsable y el encargado del tratamiento. Asimismo, el contrato debe contener una serie de cláusulas obligatorias, incluida, por ejemplo, una cláusula que estipule que el encargado del tratamiento únicamente tratará los datos personales siguiendo instrucciones documentadas del responsable del tratamiento.

Obligaciones que protegen los derechos individuales

El RGPD incluye varias obligaciones para proteger el derecho de una persona a tener control sobre sus datos personales.

Su obligación: proporcionar información transparente

Las empresas deben proporcionar a las personas información sobre quién trata qué y por qué. Como mínimo, la información debe indicar de forma clara lo siguiente:

- 👤 quién es usted,
- 👤 por qué realiza el tratamiento de datos,
- 👤 cuál es la base jurídica,
- 👤 quién recibirá los datos (si procede).

En algunos casos, la información también debe indicar lo siguiente:

- 👤 la información de contacto del DPD,
- 👤 el interés legítimo (cuando el interés legítimo sea el fundamento jurídico para el tratamiento),
- 👤 la base para la transferencia de datos a un país de fuera de la UE,
- 👤 durante cuánto tiempo se conservarán los datos,
- 👤 los derechos de protección de datos del interesado (es decir, el derecho de acceso, corrección, supresión, limitación, oposición, portabilidad, etc.),
- 👤 cómo puede retirarse el consentimiento (cuando el consentimiento es el fundamento jurídico para el tratamiento),
- 👤 si existe una obligación legal o contractual de proporcionar los datos,
- 👤 en el caso de las decisiones automatizadas, la información sobre la lógica, la importancia y las consecuencias de la decisión.

«Las empresas deben proporcionar a las personas información sobre quién trata qué y por qué».

Su obligación: derecho de acceso y derecho a la portabilidad de los datos

Las personas tienen derecho a solicitar el acceso a sus datos personales, de forma gratuita y en un formato accesible. Si usted recibe este tipo de solicitud, tendrá que hacer lo siguiente:

- 👤 informar a la persona sobre si usted está tratando sus datos personales,
- 👤 informarle sobre el tratamiento (como los fines del tratamiento, las categorías de datos de que se trate, los destinatarios de sus datos, etc.),
- 👤 proporcionar una copia de los datos personales que se estén tratando.

Además, cuando el tratamiento se basa en el consentimiento o en un contrato, las personas pueden pedir que sus datos personales se devuelvan o transmitan a otra empresa. Esto se conoce como «derecho a la portabilidad de los datos». Los datos deben proporcionarse en un formato de uso común y de lectura mecánica.

Aunque estos dos derechos están estrechamente relacionados, se trata de dos derechos distintos. Por lo tanto, usted debe asegurarse de que no haya confusión entre los dos derechos e informar a las personas en consecuencia.

Su obligación: derecho de supresión (derecho al olvido)

En determinadas circunstancias, una persona puede pedir que el responsable del tratamiento suprima sus datos personales, como cuando los datos ya no sean necesarios para cumplir el fin del tratamiento. Sin embargo, su empresa no está obligada a cumplir esta solicitud en los casos siguientes:

- 👤 el procesamiento es necesario para respetar la libertad de expresión e información de una persona,
- 👤 usted debe conservar los datos personales para cumplir una obligación legal,
- 👤 existen otras razones de interés público para conservar los datos personales, como fines de investigación científica e histórica o la salud pública,
- 👤 usted tiene que conservar los datos personales para formular una reclamación.

Su obligación: derecho de corrección y derecho de oposición

Si una persona cree que sus datos personales son incorrectos, incompletos o inexactos, tiene derecho a que se rectifiquen o completen sin dilación indebida.

Una persona también puede oponerse en cualquier momento al tratamiento de sus datos personales para un determinado uso cuando su empresa los trate basándose en su interés legítimo o para realizar una

misión en interés público. A menos que usted tenga un interés legítimo que prevalezca sobre el interés del interesado, usted deberá dejar de tratar los datos personales. Del mismo modo, una persona puede pedir que se limite el tratamiento de sus datos personales mientras se determina si su interés legítimo prevalece o no sobre el interés de dicho individuo. Sin embargo, en el caso de la mercadotecnia directa, usted siempre está obligado a dejar de tratar los datos personales a petición del interesado.

Advertencia sobre las decisiones automatizadas y la elaboración de perfiles

Las personas tienen derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado. Sin embargo, existen algunas excepciones a esta regla, como cuando la persona haya consentido explícitamente la decisión automatizada. Salvo cuando la decisión automatizada se base en una ley, su empresa debe hacer lo siguiente:

- 🔔 informar al interesado sobre las decisiones automatizadas,
- 🔔 dar al interesado derecho a que una persona revise la decisión automatizada,
- 🔔 dar al interesado la oportunidad de impugnar la decisión automatizada.

Por ejemplo, si un banco automatiza su decisión sobre la concesión de un préstamo a cierta persona, dicha persona debe ser informada de la decisión automatizada y tener la oportunidad de impugnar la decisión, así como de solicitar la intervención humana.

Obligaciones basadas en los riesgos

Además de las obligaciones para proteger los derechos individuales, el RGPD también contiene una serie de obligaciones cuya aplicación depende del riesgo.

Su obligación: nombrar un delegado de protección de datos

Un delegado de protección de datos (DPD) es el responsable de supervisar si usted cumple el RGPD. Una de las tareas fundamentales del DPD es informar y asesorar a los empleados que llevan a cabo el tratamiento real de los datos personales sobre sus obligaciones. Asimismo, el DPD colabora con la APD, actuando de punto de contacto respecto a la APD y las personas.

Su empresa debe nombrar un DPD en los casos siguientes:

- ☝ usted observa habitual y sistemáticamente a personas o trata categorías especiales de datos,
- ☝ este tratamiento es una actividad empresarial principal, y
- ☝ usted lo hace a gran escala.

Por ejemplo, si usted trata datos personales para dirigir publicidad a través de motores de búsqueda basados en el comportamiento en línea de las personas, el RGPD le exige que tenga un DPD. No obstante, si únicamente envía a sus clientes material promocional una vez al año, no necesitará un DPD. Del mismo modo, si usted es un médico que recoge datos sobre la salud de sus pacientes, probablemente no necesite un DPD. Pero si realiza el tratamiento de datos genéticos y sanitarios para un hospital, entonces sí lo necesitará.

Su obligación: protección de datos desde el diseño y por defecto

El RGPD introduce dos principios nuevos: la protección de datos desde el diseño y la protección de datos por defecto.

La **protección de datos desde el diseño** ayuda a garantizar que una empresa tenga en cuenta la protección de datos en las primeras fases de la planificación de una nueva forma de tratar los datos personales. De conformidad con este principio, un responsable del tratamiento debe tomar todas las medidas técnicas y organizativas necesarias para aplicar los principios de protección de datos y proteger los derechos de las personas. Estas medidas pueden incluir, por ejemplo, el uso de seudonimización.

La protección de datos desde el diseño minimiza los riesgos relativos a la privacidad y aumenta la confianza. Situando la protección de datos en un lugar destacado del desarrollo de nuevos bienes o servicios, puede evitarse cualquier posible problema relativo a la protección de datos en las primeras fases. Además, esta práctica ayuda a sensibilizar sobre la protección de datos en todos los departamentos y niveles de una empresa.

La **protección de datos por defecto** supone garantizar que su empresa siempre configure los parámetros por defecto de la forma más respetuosa con la privacidad. Por ejemplo, si son posibles dos configuraciones de privacidad y una de ellas impide que otros puedan acceder a los datos personales, debe utilizarse esta configuración por defecto.

«La protección de datos desde el diseño minimiza los riesgos relativos a la privacidad y aumenta la confianza».

«La protección de datos por defecto supone garantizar que su empresa siempre configure los parámetros por defecto de la forma más respetuosa con la privacidad».

Su obligación: proporcionar las debidas notificaciones en caso de violación de la seguridad de los datos

Se produce una violación de la seguridad de los datos cuando los datos personales de los que usted es responsable se difunden, accidental o ilícitamente, a destinatarios sin autorización o se impide su acceso o se alteran temporalmente.

Para una empresa, resulta vital aplicar las medidas técnicas y organizativas apropiadas con el fin de evitar

violaciones de la seguridad de los datos. Sin embargo, si se produce una violación de la seguridad de los datos y dicha violación pone en riesgo los derechos y libertades individuales, usted debe notificarla a su APD a más tardar 72 horas después de que haya tenido constancia de ella.

Dependiendo de si la violación de la seguridad de los datos supone un *alto* riesgo o no para las personas afectadas, una empresa también puede tener que informar a todas las personas afectadas por dicha violación de la seguridad de los datos.

Transferencia de datos personales fuera de la UE

EL RGPD se aplica al Espacio Económico Europeo (EEE), que incluye todos los países de la UE, más Islandia, Liechtenstein y Noruega. Cuando los datos personales se transfieren fuera del EEE, la protección que ofrece el RGPD debe viajar con los datos. Esto significa que, para exportar datos al extranjero, las empresas deben garantizar que existen determinadas garantías.

El RGPD ofrece un conjunto variado de mecanismos para transferir datos a terceros países. Según el RGPD, dichas transferencias están permitidas en los casos siguientes:

- 1.** la UE considera adecuadas las protecciones del país, o
- 2.** su empresa, por ejemplo, toma las medidas necesarias para ofrecer garantías adecuadas, como incluir cláusulas específicas en el contrato celebrado con el importador de fuera de la UE de los datos personales, o
- 3.** su empresa, por ejemplo, se basa en motivos específicos para la transferencia (llamados «excepciones»), como el consentimiento del interesado.

Para más información sobre las normas que se aplican a las transferencias internacionales de datos, consulte la Comunicación de la Comisión Europea «Intercambio y protección de los datos personales en un mundo globalizado»: <http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52017DC0007&from=ES>

¿Necesita realizar una evaluación de impacto relativa a la protección de datos?

Es obligatorio realizar una evaluación de impacto relativa a la protección de datos (EIPD) cuando el tratamiento previsto entrañe un alto riesgo para los derechos y libertades de las personas. Esto puede suceder, por ejemplo, cuando se utilizan nuevas tecnologías.

Según el RGPD, existe al menos un riesgo alto en los siguientes casos:

- 🔥 el uso de mecanismos de tratamiento automatizado y elaboración de perfiles para evaluar personas de forma sistemática y exhaustiva,
- 🔥 la observación sistemática a gran escala de una zona de acceso público (como los circuitos cerrados de televisión),
- 🔥 el tratamiento a gran escala de datos sensibles (como los datos sanitarios).

El objetivo de la EIPD es identificar los posibles riesgos para los derechos y libertades de las personas antes de que comience el tratamiento de datos personales y el riesgo se materialice. Mitigando el riesgo por adelantado, pueden evitarse daños y minimizarse costes.

Si las medidas previstas en la EIPD no eliminan todos los altos riesgos identificados, debe consultarse al DPD antes de realizar el tratamiento de datos previsto.

«Es obligatorio llevar a cabo una evaluación de impacto relativa a la protección de datos cuando el tratamiento previsto entrañe un alto riesgo para los derechos y libertades de las personas».

Qué debe hacer usted

Responder a las solicitudes

Si su empresa recibe una solicitud por parte de una persona que quiere ejercer sus derechos, usted debe responder a dicha solicitud sin dilación indebida y, en todo caso, en el plazo de un mes a partir de la recepción de la solicitud. No obstante, dicha respuesta puede prorrogarse hasta dos meses para solicitudes complejas o múltiples, siempre que se informe de la prórroga al interesado. Además, las solicitudes deben tramitarse **de forma gratuita**. Si se rechaza una solicitud, deberá informar a la persona sobre los motivos del rechazo y su derecho a presentar una reclamación ante la APD.

Demostrar el cumplimiento y llevar registros

Uno de los principios fundamentales que subyace del RGPD es garantizar que las empresas puedan demostrar su cumplimiento. Esto significa que usted debe poder demostrar que su empresa actúa de conformidad con el RGPD y cumple todas las obligaciones aplicables (en especial, a petición o por inspección de la APD).

Una forma de hacerlo es llevando registros detallados de aspectos como los siguientes:

- 👤 el nombre y los datos de contacto de su empresa relacionados con el tratamiento de datos,
- 👤 el motivo o los motivos para el tratamiento de datos personales,
- 👤 la descripción de las categorías de personas que proporcionan datos personales,
- 👤 las categorías de organizaciones que reciben los datos personales,
- 👤 la transferencia de datos personales a otro país u organización,
- 👤 el plazo de conservación de los datos personales,
- 👤 la descripción de las medidas de seguridad utilizadas durante el tratamiento de datos personales.

Además, su empresa también debe contar con procedimientos y directrices escritos, y actualizados periódicamente, y ponerlos en conocimiento de sus empleados.



CAPÍTULO 4

¿PREPARADO PARA CUMPLIRLO?

Cuando se trata del tratamiento de datos personales, el RGPD pone la pelota en su tejado. El primer paso es planear sus actividades actuales de tratamiento de datos y volver a evaluar sus procesos empresariales internos. En concreto, usted debe llevar a cabo las siguientes acciones:

- ☁ identificar qué datos posee, para qué fin y sobre qué base jurídica los posee,
- ☁ analizar todos los contratos en vigor, en especial aquellos entre responsables y encargados del tratamiento,

- ☁ evaluar todas las vías disponibles para las transferencias internacionales, y
- ☁ revisar la gobernanza general de su empresa (es decir, con qué medidas informáticas y organizativas cuenta), incluido si debe o no nombrar un delegado de protección de datos o si quiere hacerlo.

Un elemento esencial de este proceso es garantizar que el más alto nivel jerárquico de su empresa está implicado en dichas revisiones, aportando información y siendo periódicamente informado y consultado sobre los cambios de la política en materia de datos.

¿Trata datos en más de un país?

Para el tratamiento transfronterizo, puede que una autoridad de control de otro país, y no su APD nacional, sea la autoridad competente. Normalmente, es la APD

del país que alberga el establecimiento principal de su empresa (donde se adoptan las decisiones sobre los medios y fines del tratamiento) dentro de la UE.

Riesgos del incumplimiento

El incumplimiento del RGPD puede conllevar multas importantes de hasta 20 millones de euros o el 4 % del volumen de negocios total para determinadas infracciones. La APD puede imponer medidas correctivas adicionales, como ordenar el cese del tratamiento de datos personales. Asimismo, usted debe tener en cuenta el daño a su reputación que el incumplimiento podría causar.

Evidentemente, los costes de no cumplir el RGPD son mucho mayores que cualquier inversión realizada para cumplirlo.



¿Tiene alguna pregunta o duda? Póngase en contacto con su APD nacional.

Encuentre su autoridad nacional de protección de datos en línea en:

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

AVISO IMPORTANTE

La información y orientación de este folleto tienen 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 persona que actúe en su representación serán responsables del uso que pueda hacerse de la información contenida en el folleto.

El presente folleto refleja el estado en el momento de su elaboración, deberá considerarse como un «documento vivo» abierto a mejoras y su contenido puede estar sujeto a modificaciones sin previo aviso.

Ponerse en contacto con la Unión Europea

En persona

En la Unión Europea existen cientos de centros de información Europe Direct. Puede encontrar la dirección del centro más cercano en: https://europa.eu/european-union/contact_es

Por teléfono o por correo electrónico

Europe Direct es un servicio que responde a sus preguntas sobre la Unión Europea. Puede acceder a este servicio:

- marcando el número de teléfono gratuito: 00 800 6 7 8 9 10 11 (algunos operadores pueden cobrar por las llamadas);
- marcando el siguiente número de teléfono: +32 22999696; o
- por correo electrónico: https://europa.eu/european-union/contact_es

Buscar información sobre la Unión Europea

En línea

Puede encontrar información sobre la Unión Europea en todas las lenguas oficiales de la Unión en el sitio web Europa: https://europa.eu/european-union/index_es

Publicaciones de la Unión Europea

Puede descargar o solicitar publicaciones gratuitas y de pago de la Unión Europea en EU Bookshop: <https://publications.europa.eu/bookshop>

Si desea obtener varios ejemplares de las publicaciones gratuitas, póngase en contacto con Europe Direct o su centro de información local (https://europa.eu/european-union/contact_es).

Derecho de la Unión y documentos conexos

Para acceder a la información jurídica de la Unión Europea, incluido todo el Derecho de la Unión desde 1952 en todas las versiones lingüísticas oficiales, puede consultar el sitio web EUR-Lex: <http://eur-lex.europa.eu>

Datos abiertos de la Unión Europea

El portal de datos abiertos de la Unión Europea (<http://data.europa.eu/euodp/es>) permite acceder a conjuntos de datos de la Unión. Los datos pueden descargarse y reutilizarse gratuitamente con fines comerciales o no comerciales.

El Reglamento general de protección de datos (RGPD) regula la forma en que las empresas tratan y gestionan los datos personales. Gracias a una única legislación europea en materia de protección de datos, ahora su empresa debe ajustarse principalmente a una única legislación sobre protección de datos al tiempo que ofrece bienes y servicios en cualquier lugar de la Unión Europea.

Al simplificar el marco normativo para las empresas, el RGPD representa una nueva oportunidad para que su negocio mejore la gestión de los datos personales y, posteriormente, aumente la confianza de los consumidores en su empresa.

El presente folleto pone de relieve las obligaciones de su empresa en virtud del RGPD.

europa.eu/dataprotection/es

