sage

RGPD

GUÍA PARA PEQUEÑAS EMPRESAS

Información que debes conocer para adaptarte al nuevo reglamento

#IProtectData

Comparte el mensaje. Comparte la responsabilidad.

ÍNDICE

03 Introducción

04 Cómo leer esta guía

05 Aviso legal de Sage

06 Características clave del RGPD

07 El RGPD en profundidad

08 Terminología

09 Conceptos básicos sobre protección de datos

10 Principios del RGPD

13 Multas y responsabilidades

14 ¿Cumples el RGPD?

15 Preparación para el RGPD

16 Acciones inmediatas

17 De cara al futuro

18 Ejemplos del RGPD en la práctica

19 Ventas y marketing

21 Recursos humanos y nóminas

22 Contabilidad y finanzas

23 Tecnología de la información

25 Preguntas y respuestas sobre el RGPD

INTRODUCCIÓN

El Reglamento General de Protección de Datos (RGPD) se considera la mayor reestructuración relacionada con la forma de recopilar, almacenar y usar los datos de las personas.

Sus implicaciones son enormes y casi con seguridad muchas empresas aún no las han asimilado, a pesar de que la legislación entra en vigor el 25 de mayo de 2018.

El RGPD va mucho más allá de la legislación sobre protección de datos existente (en el caso de España, la actual LOPD), y afecta a empresas de todos los tamaños, desde comerciantes independientes hasta las mayores corporaciones. El estudio realizado por Sage* revela que el 52 % de las empresas en España no es consciente del RGPD, mientras que el 37 % no comprende lo que el RGPD significa para su empresa.

Afectará a la forma de hacer negocios, como el área de marketing, y a la forma de abordar cuestiones como el personal y los datos internos en relación con la gestión de la empresa.

Con la perspectiva de incurrir en multas de hasta el 4 % del volumen de negocio anual en todo el mundo o de 20 millones de euros, la que sea de mayor cuantía, conocer el RGPD no es algo opcional. Cabe destacar que se podrán aplicar multas por una violación del reglamento, aunque no se haya producido una pérdida de datos real.

El objetivo de este documento es servir de guía breve para ayudar a las empresas a prepararse para la implementación del RGPD, pero no puede sustituir a una auditoría completa llevada a cabo por un profesional con la cualificación adecuada. Lee el Aviso legal de Sage en la página 05.

*Encuesta a clientes sobre el RGPD, octubre de 2017

> Simplemente es una nueva legislación. Se puede establecer un plan, implementar algunas nuevas medidas y continuar con el trabajo diario. No hay que dejarse llevar por el pánico. Sin embargo, no podemos ignorarla.

Orlagh Kelly

Abogada y directora general de Briefed, especialistas en formación y cumplimiento del RGPD

CÓMO LEER ESTA GUÍA

Esta guía contiene varias secciones distintas y puedes empezar a leer la que te parezca más adecuada.

Para ver un examen en profundidad del RGPD, echa un vistazo a la página **07**

Haz clic aquí para ver

Para averiguar cuál podría ser tu próxima línea de acción, echa un vistazo a la página **15**

Haz clic aquí para ver

Para ver respuestas a preguntas habituales formuladas por empresas acerca del RGPD, echa un vistazo aquí **25**

Haz clic aquí para ver

AVISO LEGAL DE SAGE

La información contenida en esta guía es meramente orientativa. Ni está pensada como asesoramiento legal ni debe tomarse como tal. Nos gustaría resaltar que los clientes deben llevar a cabo su propia investigación minuciosa o buscar asesoramiento legal si no están seguros de las implicaciones del RGPD para sus empresas.

Si bien hemos intentado que la información facilitada en esta guía sea correcta y esté al día, Sage no garantiza su precisión o exhaustividad y la proporciona "tal cual", sin ningún tipo de garantía, ni explícita ni implícita. Sage no aceptará ninguna responsabilidad por los posibles errores u omisiones ni por los daños (incluidos, sin limitación, las pérdidas de actividad o el lucro cesante) producidos dentro o fuera de un contrato o por el uso o confianza en esta información o por alguna acción o decisión tomada como resultado del uso de la misma.

CARACTERÍSTICAS CLAVE DEL RGPD

Reglamento General de Protección de Datos (RGPD)

Derechos del individuo

Amplía los derechos de las personas físicas y la información que deben recibir sobre el tratamiento de sus datos.

Consentimiento

Debe ser una declaración u otra acción afirmativa clara. o se puede dar por supuesto ni siquiera usar casillas ya marcadas en una web.

Delegado de Protección de Datos

Ha de ser obligatorio. Debe estar especializado en la legislación de protección de datos. Puede ser empleado o subcontratado.

Sanciones

Pueden llegar al 4 % de la facturación anual mundial o 20 millones de euros, lo que sea mayor. La sanción puede imponerse, aunque no haya pérdida en sí de los datos.

Privacidad de principio a fin

La privacidad debe tenerse en cuenta en todo y solo pueden usarse los datos estrictamente necesarios para el fin estipulado.

Portabilidad de los datos

Las personas tienen ahora el derecho a mover, copiar o transferir sus datos, incluso a una empresa de la competencia.

Ámbito de aplicación mayor

Afecta a las empresas y a quienes se encarguen del tratamiento de datos para ellas, incluso fuera de la UE.

Comunicación obligatoria de las violaciones de la seguridad

Los responsables de los datos deben informar a la autoridad de control (la AEPD en España) en el plazo de 72 horas desde su conocimiento. En violaciones graves de la seguridad, hay que informar a los interesados.

Fuente: Reglamento General de Protección de Datos (RGPD): Guía rápida de Sage para empresas

EL RGPD EN PROFUNDIDAD

Esta es una breve introducción sobre los conceptos y términos clave del RGPD.

Terminología

Aunque pueda resultar sorprendente, empezar a abordar el RGPD no exige necesariamente comprender la jerga legal y una terminología compleja. Sin embargo, hay algunas excepciones relacionadas con los términos que conviene aprender cuanto antes porque deberás utilizarlos en tu propia documentación de cumplimiento del RGPD.

El RGPD identifica funciones claras que determinan los parámetros relacionados con la forma de tratar los datos personales y, por tanto, lo que se le exige. Como empresa necesitas saber cuál de estas funciones es la tuya:

Responsable de tratamiento de datos: la persona, autoridad pública, agencia o cualquier otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento de datos personales. Si recopilas datos personales para tu propio uso y fines, tú eres el responsable y eres plenamente responsable del cumplimiento del RGPD, lo que incluye toda la seguridad.

Encargado de tratamiento: una persona, autoridad pública, agencia o cualquier otro organismo que realiza el tratamiento de datos personales en nombre de un responsable. Si procesas datos personales en nombre de otra organización, tú eres el encargado del tratamiento y solo debes actuar siguiendo las instrucciones de la organización de control. Sin embargo, también eres responsable por cualquier obligación de cumplimiento del RGPD impuesta a los encargados de tratamiento.

Responsables conjuntos, o responsables en común: en ocasiones puede haber responsables conjuntos, cuando dos o más responsables deciden los datos personales que se recopilan y para qué se utilizan. Por ejemplo, un fabricante puede compartir datos de clientes con sus minoristas porque ambos comparten el interés en estos datos. También puede haber responsables en común, cuando dos o más responsables comparten los mismos datos, pero los procesan de forma independiente entre sí. Por ejemplo, un contable o gestor de cuentas puede ser un responsable en común contigo porque tiene que procesar los datos de tus clientes como parte del proceso contable.

El caso habitual sería que el encargado de tratamiento sea un tercero contratado por el responsable.

Una de las novedades del RGPD es el hecho de que tanto los responsables como los encargados de tratamiento son responsables de las violaciones que afectan a los datos personales. Sin embargo, los responsables deben garantizar que los encargados de tratamiento proporcionen "garantías suficientes" de que se cumplirá el RGPD, y que se protegerán los derechos de los datos de las personas. Un responsable debe utilizar un contrato por escrito al emplear a un encargado de tratamiento.

También es necesario comprender lo que entendemos por datos personales y un interesado.

Interesado: este es el término que el RGPD utiliza para referirse a una persona física identificada o identificable a la que se puede hacer referencia utilizando lo que se consideran datos personales (véase más abajo).

Datos personales: incluye, entre otros, un nombre, un número de identificación, datos de ubicación o un identificador en línea, o uno o varios factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de dicho individuo.

Categorías especiales de datos: se trata de datos que revelan el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas o la afiliación sindical, y el procesamiento de datos genéticos, datos biométricos con el fin de identificar de manera inequívoca a una persona física, datos sanitarios o datos relacionados con la vida sexual o la orientación sexual de una persona física, y suscitan una mayor protección.

Por último, es importante aclarar a qué nos referimos cuando hablamos de tratamiento de datos.

Tratamiento: cualquier operación o conjunto de operaciones, incluidas las efectuadas mediante procedimientos automatizados y aplicadas a datos personales, como la recogida, registro, organización, estructuración, almacenamiento, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, así como su restricción, eliminación o destrucción.

Los términos anteriores se utilizan en toda esta guía.

Conceptos básicos de protección de datos

El RGPD se basa en los principios de protección de datos existentes con los que, como empresa, ya deberías estar familiarizado. Se resumen de la siguiente manera:

Principios de protección de datos

Los datos personales serán tratados de manera lícita, leal y transparente en relación con la persona interesada. Se deben recopilar con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines.

Los datos personales que se recojan deben ser adecuados, pertinentes y limitarse a lo que es necesario. Deben ser exactos y mantenerse actualizados, y se tomarán todas las medidas razonables para la supresión o rectificación sin demora de los datos personales que sean inexactos. Se deben almacenar de manera que identifiquen a la persona solo el tiempo que sea necesario, y se deben procesar de forma que se garantice la seguridad adecuada, incluida la protección contra pérdida, destrucción o daños, y el acceso no autorizado o ilícito.

Tratamiento lícito

El tratamiento de datos personales solo es lícito si se aplica al menos una de las condiciones siguientes:

1. La persona ha dado su consentimiento para uno o más fines determinados
2. Es necesario para un contrato en el que la persona es una parte interesada, o lo será en breve
3. Es necesario para cumplir una obligación legal (p. ej., presentación de registros fiscales por parte de una empresa)
4. Se trata de una tarea de interés público o que se lleva a cabo en interés de un poder público
5. Es necesario para proteger los intereses vitales de la persona interesada o de otra persona física (situaciones de vida o muerte)
6. Es necesario para los intereses legítimos del responsable (o los de un tercero) salvo cuando prevalezcan los intereses, derechos fundamentales y libertades de la persona

Transferencias internacionales

El RGPD mantiene la prohibición general de enviar datos personales fuera del Espacio Económico Europeo a un país u organización que no proporcione la protección adecuada para los datos personales. Durante la redacción de este documento, los países y organizaciones que la Comisión Europea considera que proporcionan una protección "adecuada" son: empresas estadounidenses que autocertifican el acuerdo del Escudo de Privacidad entre la UE y los EE. UU. (nota: no significa que se considere que los EE. UU. como país proporcionan una protección adecuada), Andorra, Argentina, Canadá (con limitación a la legislación canadiense relacionada con la privacidad de los datos, conocida como PIPEDA), islas Feroe, Guernesey, Israel, Isla de Man, Jersey, Nueva Zelanda, Suiza y Uruguay. En los lugares donde no existe una decisión sobre el carácter adecuado de la protección, las transferencias solo se pueden realizar en circunstancias limitadas, lo que incluye basarse en el consentimiento, el uso de cláusulas contractuales estándar publicadas por la Comisión Europea o, en el caso de transferencias entre empresas, el uso de normas empresariales vinculantes.

Principios del RGPD

El RGPD se basa en los principios básicos de las siguientes formas y su objetivo es proporcionar una norma mínima para la protección de datos.

Expansión del ámbito y el área geográfica

Anteriormente solo los responsables eran directamente responsables por las violaciones que afectaban a los datos personales. Según el RGPD, ahora tanto los responsables como los encargados de tratamiento son responsables.

Además, no solo se ven afectados los responsables y los encargados de tratamiento en la UE, sino también los que se encuentran fuera de la UE y que ofrecen bienes o servicios a personas de la UE, sin importar si se requiere el pago; o bien que supervisan el comportamiento de personas en la UE.

Es posible que estas empresas tengan que designar a un representante de la UE para cumplir el RGPD en su nombre si su tratamiento de datos personales es frecuente, o incluye el tratamiento a gran escala de categorías especiales de datos, o implica el tratamiento de datos relacionados con categorías especiales de datos.

Responsabilidad proactiva y mantenimiento de registros

Según el RGPD, los responsables deben ser capaces de demostrar que cumplen la norma. Esto se logra parcialmente cumpliendo una serie de exigencias sobre registros bastante costosas. En concreto, se deben mantener registros en los que se detallen:

1. Actividades de tratamiento (si emplean a más de 250 personas, o menos en los casos en que sea probable que el tratamiento realizado suponga un riesgo para los derechos y libertades de las personas, no son ocasionales, o incluyen categorías especiales de datos)
2. Solicitudes de consulta de datos de un sujeto
3. Violaciones
4. Cómo se obtienen los consentimientos
5. Evaluaciones de impacto sobre la intimidad (véase más abajo).

También se exige que los encargados de tratamiento mantengan registros de sus actividades de tratamiento, aunque los requisitos no son tan detallados como en el caso de los responsables.

Privacidad desde el diseño y por defecto

Se trata de dos nuevos conceptos clave presentados con el RGPD.

La privacidad desde el diseño significa que cualquier actividad que pueda afectar a las expectativas de privacidad de las personas debe tenerse en cuenta en cada etapa de cualquier actividad de tratamiento, desde la concepción hasta la ejecución y finalmente el cese de esa actividad. Esto se puede demostrar mediante la formación continua, llevando a cabo auditorías periódicas, restringiendo el acceso a los datos personales en función de la necesidad de conocimiento e implementando medidas de seguridad técnicas y organizativas adecuadas como la seudonimización y el cifrado.

El RGPD también exige que se lleven a cabo evaluaciones de impacto sobre la intimidad cuando exista un riesgo alto para los datos personales. Se trata de un proceso sistemático, normalmente un cuestionario, para evaluar los posibles efectos sobre la privacidad de un proyecto, iniciativa o bien sistema o esquema propuesto de las personas.

La privacidad por defecto requiere que se implementen medidas de seguridad técnicas y organizativas adecuadas para garantizar por defecto que solo se realice el tratamiento de los datos personales que sean necesarios para el tratamiento (denominado “minimización de los datos”).

Comunicación obligatoria de las violaciones de la seguridad

Los responsables deben notificar a las autoridades de control, como la Asociación Española de Protección de Datos (AEPD) en España, en un plazo de 72 horas desde el conocimiento de una violación. Si esa violación implica un riesgo alto para las personas implicadas, los responsables también deben notificar a las personas afectadas sin retraso injustificado. Los encargados de tratamiento deben notificar a los responsables cualquier violación sin retraso injustificado.

Obtener el consentimiento de los clientes

Tal como se ha mencionado anteriormente (véase Tratamiento lícito en la página 9), el consentimiento es solo un medio de garantizar que los datos personales se protegen legalmente. Por ejemplo, si ya ha suscrito un contrato con una persona, o si lo va a hacer en breve, no es necesario el consentimiento.

Sin embargo, e igual que anteriormente, cuando se exige el consentimiento debe entregarse de manera libre, específica, informada e inequívoca.

Según el RGPD, también se debe confirmar mediante una declaración u otra acción afirmativa clara, lo que significa que la ausencia de confirmación, las casillas ya marcadas en páginas web y la inactividad ya no pueden constituir un consentimiento. Decir "sí" durante una llamada telefónica puede contar como un consentimiento, aunque se deben conservar registros.

Debido a que con la nueva norma el consentimiento debe ser específico, el RGPD establece expresamente que no puede ser "agrupado".

Es decir, son necesarios consentimientos independientes para distintas operaciones de tratamiento de datos.

Por último, se debe informar a las personas de que tienen derecho a retirar su consentimiento en cualquier momento y debe resultarles tan sencillo retirar el consentimiento como lo fue otorgarlo.

Derechos de sus clientes

Sus clientes (es decir, los interesados) tienen derecho a que se les proporcione información sobre lo que usted hace con sus datos personales. De hecho, el RGPD exige que los responsables proporcionen incluso más información que la que se exigía en comparación con la normativa anterior. La información sobre estos derechos se suele entregar en forma de un "aviso de privacidad", a menudo en un sitio web, pero se debe mantener un procedimiento transparente en todo momento.

En concreto, se debe informar a las personas de que tienen los siguientes derechos (entre otros):

1. A la queja ante las autoridades de control
2. A la retirada del consentimiento al tratamiento de sus datos personales
3. Al acceso a sus datos personales, así como a su rectificación o supresión ("el derecho al olvido")
4. Al conocimiento de la existencia de cualquier tratamiento automatizado (incluida la elaboración de perfiles)
5. A la oposición a ciertos tipos de tratamiento, como por ejemplo el marketing directo o las decisiones basadas únicamente en un tratamiento automatizado
6. A ser informadas de cuánto tiempo se conservarán los datos personales
7. Y a conocer los datos de contacto de los Delegados de Protección de Datos designados (DPD).

Las personas también tienen el derecho de "portabilidad de dato"», es decir, a que se les devuelvan los datos personales automatizados que el interesado proporcionó al responsable a partir del consentimiento o contrato, o a que se envíen directamente a otro responsable. Podría tratarse incluso de su competencia, pero no crea que puede dificultarles su uso; los datos personales se deben enviar en un formato estructurado, de uso común y legible por medios electrónicos, para que sea posible mover, copiar o transferir los datos personales entre distintos entornos de TI.

Delegado de Protección de Datos

Según el RGPD, los responsables y también los encargados de tratamiento deben designar a un Delegado de Protección de Datos (DPD) cuando:

(i) El tratamiento lo lleve a cabo una autoridad u organismo público, excepto en el caso de juzgados que actúen en su capacidad judicial

(ii) Las actividades principales del responsable o el encargado de tratamiento consistan en operaciones de tratamiento que, por su naturaleza, su ámbito y/o sus fines, exijan la supervisión sistemática de personas a gran escala

(iii) Las actividades principales del responsable o el encargado de tratamiento consistan en el tratamiento a gran escala de categorías especiales de datos y datos personales relacionados con condenas e infracciones penales.

Su DPD puede ser un empleado o puede recurrir a un tercero, pero debe notificar a la autoridad supervisora local la identidad del DPD.

El trabajo del DPD consistirá en informar a la empresa y a su personal de sus obligaciones según el RGPD. También deberá supervisar el cumplimiento del RGPD (y de cualquier otra ley o requisito de protección de datos), como por ejemplo gestionar evaluaciones de impacto de protección de datos, realizar auditorías internas y organizar la formación del personal. El DPD también será el primer punto de contacto para consultas relacionadas con la protección de datos procedentes de las autoridades de control, y el punto de contacto para cualquier persona cuyos datos trate la empresa, incluidos clientes y empleados.

“La mejor forma de poner en marcha el proyecto es recurrir a un experto para que lleve a cabo un análisis de deficiencias, ya que de esa forma se harán patentes todos los problemas, se destaparán todas las cuestiones y se les asignará una metodología o un orden, para abordarlos posteriormente.”

Creo que muchas empresas están sorprendidas por la profundidad del RGPD y la amplitud de implantación que tendrá en su negocio y en los distintos departamentos.

Un error de concepto importante sería que de este tema debe encargarse el departamento de TI, algo totalmente incorrecto. En realidad, toda la empresa debe implicarse. Todo el mundo debe recibir formación para comprender lo que pueden hacer y lo que no.

Orlagh Kelly

Abogada y directora general de Briefed, especialistas en formación y cumplimiento del RGPD

Multas y responsabilidades

Tal como se ha mencionado anteriormente, si infringes el RGPD puedes enfrentarte a multas administrativas de hasta el 4 % del volumen de negocio anual en todo el mundo o de 20 millones de euros, la que sea de mayor cuantía. Esto se aplica tanto a los responsables como a los encargados de tratamiento.

Las autoridades de control serán responsables de investigar las violaciones de datos u otras infracciones del RGPD, y tendrán capacidad de aplicar multas. Según el ICO, todas las multas se trasladan directamente al Gobierno.

¿CUMPLES EL RGPD?

Según el RGPD existen seis bases jurídicas para la gestión y el tratamiento de los datos personales de individuos, que son las siguientes. Se debe aplicar al menos una.

Intereses legítimos	Se trata de un área subjetiva y las empresas deben equilibrar su derecho a usar los datos de una persona con el derecho de la persona a que no se usen sus datos. Las empresas deben tener una motivación clara y contundente para explicar los motivos por los que se deben usar los datos de una persona y la práctica recomendada sería documentar el razonamiento que respalda la decisión.
Consentimiento	El consentimiento debe entregarse de manera libre, informada e inequívoca, y se puede capturar en distintos formatos (p. ej., en línea mediante una casilla de verificación), o respondiendo "sí" en una llamada telefónica, aunque se debe conservar un registro de este consentimiento.
Contrato	Está relacionado con el procesamiento necesario de datos personales como parte de un contrato del que el interesado forma parte, o bien para realizar acciones a petición del interesado antes de cerrar un contrato, y no varía respecto a los reglamentos de protección de datos actuales.
Obligación legal	Entre los ejemplos de obligaciones legales se incluyen las que se producen como parte del cumplimiento fiscal con la administración fiscal y aduanera o con fines de prevención de fraudes según reglamentos financieros.
Intereses vitales	Una organización permite el tratamiento de datos personales para proteger los intereses vitales de la persona interesada. Básicamente, este punto está relacionado con situaciones de "vida o muerte".
Interés público	Se aplica en caso de que sea necesario procesar datos personales por el interés público, por ejemplo, en relación con la realización de tareas llevadas a cabo por una autoridad pública.

PREPARACIÓN PARA EL RGPD

A continuación, se incluyen sugerencias de pasos a seguir que puedes tener en cuenta. Recuerda que las medidas de preparación para el RGPD suelen clasificarse en dos categorías: gestionar cuestiones internas, como garantizar que el tratamiento de los datos de los empleados cumple la norma, y gestionar cuestiones externas, como garantizar que la gestión de los datos de los clientes cumple la norma. Ninguna es más importante que la otra, y es necesario abordar ambas.

Acciones inmediatas

A continuación se incluyen algunas medidas que deberías valorar poner en marcha cuanto antes

Informar al personal y a los proveedores

Es improbable que cualquier miembro del personal de la empresa no se vea afectado por los efectos del RGPD, ya sea en la forma de realiza su trabajo o en cómo la empresa lo tratará una vez que se aplique el RGPD. Deberías empezar por informar a los empleados de los cambios probables que se avecinan. Podrías solicitar que el personal lleve a cabo su propia investigación para averiguar cómo se verán afectadas sus funciones, especialmente si pertenecen a un sindicato u organismo comercial que pueda asesorar sobre el RGPD.

Cualquier empresa o agencia externa con la que colabores también deberá cumplir el RGPD, así que deberás iniciar conversaciones al respecto con ellas.

Identificar

Adopta el enfoque de averiguar qué, cuándo, dónde, porqué y cómo. Es probable que todas las funciones de una empresa se vean afectadas por la exigencia de tratamiento lícito del RGPD. Debes hacer una lista de las áreas de tu empresa que necesitarán atención y en las que deberás centrarte, para así crear un cronograma de aplicación de los cambios.

En función de la estructura de tu empresa, podrías hablar con los responsables de cada departamento y pedirles que creen planes de implementación del RGPD.

Revisar los datos que ya tienes

Consulta los datos en cada una de las funciones de tu empresa. Recuerda que los datos pueden adoptar todo tipo de formatos. Aunque las bases de datos de clientes pueden ser el objetivo de revisión obvio, los correos electrónicos e incluso los mensajes de textos también pueden formar parte del ámbito del RGPD.

Echa un vistazo a tu lista de clientes. ¿Cuentas con una base jurídica para procesar los datos personales de cualquier persona incluida en ella (véase la página 14 para recibir orientación)? Si la respuesta es no, ¿qué planes vas a establecer para lograr esa base jurídica?

Investigación

Cada vez hay más datos disponibles acerca del RGPD, pero debes asegurarte de consultar también la información proporcionada por las autoridades de control.

Tal vez descubras que otras personas de tu mismo ámbito empresarial han compartido en la red sus experiencias de implementar el RGPD. Esto podría proporcionarte información útil y vital para tu negocio.

De cara al futuro

A continuación, se muestran algunas tareas y objetivos de implementación tras el análisis inmediato de los requisitos del RGPD.

Obtener una auditoría del RGPD

Aunque podrías decidir auditar el cumplimiento del RGPD en tu propia empresa, el carácter especializado de la tarea junto con el tiempo necesario para desarrollarla hacen que resulte más adecuado ponerla en manos de una persona con la cualificación necesaria que elaborará un informe en el que se detallen los pasos necesarios.

Existen varios tipos de consultorías del RGPD y, en función de la naturaleza y el tamaño de tu empresa, puede que necesites realizar más de una consulta.

Aparentemente, algunas empresas ofrecen auditorías completas del RGPD centradas en tecnología de la información y, aunque en definitiva se trata de una parcela importante, el RGPD también requerirá formar al personal y puede que un cambio cultural global en la empresa a la hora de tratar con los clientes. Por lo tanto, debes asegurarte de encontrar a un auditor (o auditores) que se ajuste a todas tus necesidades. Echa un vistazo a la página 13.

Designar un DPD

Si tu empresa necesita un Delegado de Protección de Datos (véase la página 11), deberás designarlo. Puede ser un miembro de tu personal actual, una incorporación a la plantilla o alguien de una agencia externa. En todo caso, deberás notificar a la autoridad supervisora local su identidad.

Comunicar información privada

Debes revisar tus avisos de privacidad actuales y establecer planes para realizar los cambios necesarios a tiempo. El RGPD incluye requisitos adicionales de presentación de información a los clientes al procesar sus datos (véase Derechos de tus clientes en la página 11).

Configurar procedimientos de respuesta al RGPD

El RGPD establece un requisito legal para que los responsables notifiquen las violaciones en un plazo de 72 horas desde que tengan conocimiento de ellas, por lo que deberás poner a disposición de los empleados los recursos necesarios para hacerlo, así como los recursos para garantizar la supervisión constante del proceso. Si cuentas con un DPD, esto formará parte de sus competencias.

Debido a que el RGPD permite a las personas tomar medidas como retirar su consentimiento para que se procesen sus datos personales, o para acceder a sus datos y eliminarlos o transferirlos, entre otras, deberás asegurarte de que siempre exista la infraestructura necesaria para gestionar estas solicitudes. Una vez más, un DPD se encargará de ello si tu empresa debe contar con uno.

Revisión y supervisión

A diferencia de la anterior legislación sobre protección de datos, la implementación del RGPD no es un proceso puntual. El RGPD exige a las empresas que se garantice la implementación de la privacidad desde el diseño y por defecto, lo que significa que todos los nuevos procesos, sistemas y otros elementos deberán desarrollarse teniendo en cuenta los requisitos del RGPD.

Deberás evaluar a cualquier encargado externo que colabore con tu empresa para confirmar que cumple el RGPD, ya que el RGPD le asigna esta responsabilidad, y puedes decidir implementar, por ejemplo, auditorías periódicas de estos colaboradores externos.

Comprender las responsabilidades internacionales

Si tu empresa opera en más de un Estado miembro de la UE, debes determinar y documentar dónde se encuentra su autoridad supervisora de protección de datos principal.

EJEMPLOS DEL RGPD EN LA PRÁCTICA

El RGPD se basa en los principios básicos de las siguientes formas y su objetivo es proporcionar una norma mínima para la protección de datos.

Ventas y marketing

Los nuevos requisitos más estrictos del RGPD sobre el consentimiento pueden afectar a los procesos de marketing y clientes de manera especialmente dura.

A continuación, se muestran algunos ejemplos sobre cómo el RGPD afectará a una pequeña empresa, con las siguientes salvedades. Primero, no se trata de una lista exclusiva ni sustituye la necesidad de obtener asesoramiento jurídico competente o examinar tus propios procedimientos y métodos en profundidad (véase el Aviso legal en la página 5).

Segundo, durante la redacción de este documento aún se desconoce el impacto exacto del RGPD. Por ejemplo, carecemos de ejemplos prácticos sobre lo que es probable que las autoridades supervisoras consideren aceptable u objetable, y parte de la redacción de la legislación sobre el RGPD es susceptible de interpretación. Por lo tanto, la información que se describe en este documento solo puede considerarse, como mucho, suposiciones.

Datos de marketing existentes

En pocas palabras, con las bases de datos existentes de contactos de marketing deberás realizar, como mínimo, dos tareas antes de la implementación del RGPD:

1. Revisar jurídicamente el consentimiento que se utilizó inicialmente y confirmar si es compatible con los requisitos del RGPD (véase Derechos de tus clientes en la página 11).
2. En el caso probable de que el consentimiento existente sea insuficiente, y que no exista otra base para el tratamiento lícito de los datos (véase Tratamiento lícito en la página 9), deberás ponerte en contacto con cada una de las personas de la base de datos y solicitar un nuevo consentimiento. Si no obtienes el consentimiento nuevo y concreto para las formas en que deseas procesar los datos, la información de esa persona deberá suprimirse o eliminarse.

Se ha calculado que los requisitos anteriores podrían implicar que bases de datos como las de ventas y marketing se reduzcan hasta en tres cuartas partes. Sin embargo, también se ha señalado que los clientes que proporcionan el nuevo consentimiento demuestran ser más valiosos por su disposición a colaborar con la empresa.

Recuerda que el consentimiento es solo uno de los posibles requisitos del tratamiento lícito (véase Tratamiento lícito en la página 9). Si ya existe un contrato en curso con un cliente, o si es probable que exista pronto, no será obligatorio obtener el consentimiento, por ejemplo, si dicho tratamiento es necesario para la ejecución de un contrato o en el interés legítimo de tu empresa o el cliente.

Consentimiento de cara al futuro

Por supuesto, deberás crear nuevos procesos compatibles con el RGPD para cualquier dato personal que recopiles de las personas a partir de ahora, lo que puede implicar obtener el consentimiento.

Recuerda que ya no puedes suponer el consentimiento, ni utilizar un consentimiento único como carta blanca para todas las actividades de tratamiento, ni usar una casilla ya marcada en un sitio web para asumir que se ha proporcionado el consentimiento (véase Obtener el consentimiento de los clientes en la página 11).

Antes de adquirir contactos de marketing, deberás asegurarte de que el consentimiento de cada persona incluida cumple el RGPD, es decir, que cada una de ellas ha proporcionado un consentimiento claro e individual para que sus datos se comercialicen de esta forma. Teniendo en cuenta que es improbable que la mayoría de la gente acepte esto, es probable que la venta, compra o transferencia de contactos de marketing se convierta en una actividad excepcional.

Minimización de los datos

El RGPD establece que las empresas no pueden simplemente recopilar muchos datos de una persona sin justificación (véase Privacidad desde el diseño y por defecto en la página 10), por lo que el marketing va a dejar de ser una "expedición de pesca" en la que se presentan casillas o un cuestionario con objeto de poder usar de alguna forma los datos recopilados en el futuro. En tus procesos deberán figurar qué datos se recopilan y se deberá explicar el uso previsto para ellos, y puede que necesites obtener el consentimiento para usar esos datos de una forma concreta. También deberás documentar el momento en el que tienes previsto suprimirlos o borrarlos.

Gestión de las consultas de clientes

Tal como se menciona en la página 11, el RGPD otorga a sus clientes nuevos derechos para saber lo que pasa con sus datos. También tienen el derecho de retirar el consentimiento, con ciertas excepciones, o el derecho absoluto de retirar el consentimiento en relación con determinados usos (como el marketing directo). Deberás establecer procedimientos y posiblemente personal que se encargue de esta gestión, como un DPD (véase la página 11), y tu personal deberá realizar tareas como documentar dichas solicitudes y filtrar las listas de marketing futuras con esta lista de supresión interna.

Recursos humanos y nóminas

Teniendo en cuenta que la gestión del personal y de las nóminas implica procesar enormes cantidades de datos personales, es muy improbable que no sea necesario revisar considerablemente los procesos existentes para el RGPD.

Consolidación y seguridad

Con sus requisitos de seguridad adicionales, las empresas deben consolidar todos los datos de su plantilla y relacionados con nóminas en las menores ubicaciones posibles como parte de la preparación para el RGPD. Esto forma parte del requisito de protección de los datos (véase Privacidad desde el diseño y por defecto en la página 10). Por ejemplo, es probable que la protección eficaz de los datos del personal y los datos de las nóminas repartidos por distintas hojas de Excel acabe en desastre.

Las empresas de mayor tamaño también deben asegurarse de que cumplen las reglas y normas relevantes, como la ISO 27001, que facilitará la implementación del RGPD.

Los procesos conformes con el RGPD que cree deberán tener en cuenta todas las fuentes de datos, lo que puede suponer un desafío con la gestión del personal. Por ejemplo, ¿cómo almacenarás de manera segura los justificantes médicos o incluso los correos electrónicos o mensajes de texto en los que se soliciten días de vacaciones? ¿Cómo se pueden gestionar y almacenar de forma segura los partes de horas? ¿Cómo puedes restringir el acceso a los datos personales para garantizar que solo puedan acceder a ellos las personas que tengan una "necesidad de conocer"?

Asimismo, e igual que anteriormente, las nóminas deben proporcionarse de manera segura. Este requisito está fomentando que muchas empresas cambien al formato electrónico en lugar de usar nóminas en papel, ya que los empleados deben autenticarse online de manera segura antes de poder ver la información.

Los derechos del individuo

Debido a que el empleado tiene un contrato con su empresa, y a que tú estás procesando sus datos basándote en el contrato de trabajo o para tus intereses legítimos, no es necesariamente apropiado obtener el consentimiento en la relación diaria entre el empleador y el empleado. Sin embargo, puede que necesites el consentimiento del empleado para cualquier tratamiento no conectado directamente con esa relación, p. ej., si deseas ver los datos sobre salud en el trabajo de un empleado. Esto incluye el consentimiento para datos confidenciales, aunque en este caso el RGPD se supedita a la legislación nacional. Durante la redacción de este documento aún no están totalmente claras las implicaciones asociadas.

El RGPD implica que puede que tengas que ofrecer a tu personal visibilidad completa de los datos que posees sobre ellos. Deberás responder a solicitudes de consulta de datos de un sujeto. Cabe señalar que conservas el derecho de rechazar solicitudes excesivas o infundadas, pero deberás demostrar en qué sentido son infundadas en su documentación de cumplimiento.

Deberás redactar avisos de privacidad claros y que cumplan el RGPD para garantizar que proporciona toda la información a la que tengan derecho según el requisito de transparencia del RGPD. Puede que tengas que proporcionar capacidades de acceso sencillo para permitir a los empleados excluirse de las distintas formas en que usas sus datos. No podrás usar sus datos para ningún otro fin sin notificárselo.

Selección de personal

Desde el momento en que un empleado potencial envíe un curriculum (CV) o formulario de solicitud, deberás empezar a registrar cuándo y cómo has obtenido estos datos y en función de qué base jurídica los conservas.

Los CV no solicitados recibidos de demandantes de empleo también suponen un reto, ya que los departamentos de recursos humanos no podrán conservarlos a menos que puedan vincularlos con un registro claro de consentimiento que incluya un límite de tiempo acordado. Tal vez debas plantearte solicitar el consentimiento explícito de los candidatos para archivar sus CV durante un periodo de tiempo. Tal como se indica anteriormente, también deberás proporcionar avisos de cumplimiento del RGPD claros a los demandantes de empleo.

Eliminación de los datos

El RGPD establece que no deberías conservar los datos de un empleado una vez que este deje la empresa a menos que exista un motivo lícito para ello. Esta cuestión debe tenerse en cuenta como parte del derecho al olvido, como se menciona en la página 11 (véase Derechos de tus clientes), pero no se trata de un derecho absoluto si hay un motivo lícito para que la empresa conserve los datos. Por ejemplo, si un antiguo empleado ha presentado una demanda laboral contra tu empresa, deberás conservar esos datos.

Sin embargo, deberá asegurarse de que sus sistemas y procesos son capaces de eliminar todos los datos sobre ese individuo, lo que sugiere otro motivo para buscar la consolidación de los datos en el menor número de sistemas posible.

Contabilidad y finanzas

De todos los departamentos de una empresa, el de contabilidad es quizás el menos afectado por los preparativos y requisitos del RGPD. La norma general es que, a menos que los datos contables estén vinculados a una persona, no debería haber problema.

Si los datos contables están vinculados a una persona, en la mayoría de los casos ya tendrás un contrato con ella (por ejemplo, un contrato de ventas), y se procesarán los datos con fines de contabilidad para los intereses legítimos tanto de dicha persona como de la empresa.

Si existe la necesidad de obtener el consentimiento para usar los datos de una persona, se debe especificar el requisito de procesamiento con fines contables durante la obtención del consentimiento. Esto puede implicar que el contable o el equipo de contabilidad se ponga en contacto con todos los departamentos para garantizar el cumplimiento del RGPD hacia los niveles superiores.

Pero podrían surgir problemas si contratas a un gestor de cuentas o empresa de contabilidad en cualquier función. Deberás asegurarte de que cumplen el RGPD, que la tecnología y el software que usan son compatibles con el RGPD, y que la forma y la ubicación en que almacenan los datos también cumplen el RGPD.

Tecnología de la información

Los departamentos de TI son los facilitadores de gran parte del cumplimiento del RGPD teniendo en cuenta que la mayor parte del trabajo que realiza una empresa actualmente se lleva a cabo usando tecnología. Por ejemplo, con el creciente uso de los servicios en la nube, el departamento de TI deberá asegurarse de que cualquier ubicación en la que se almacenen datos cumpla los requisitos de seguridad exigidos por el RGPD.

Sin embargo, no se trata necesariamente de proporcionar software o hardware para la preparación del RGPD. Es posible que el departamento de TI tenga que desechar de manera segura datos existentes, como las bases de datos de clientes que carezcan de notificaciones de consentimiento adecuadas, y establecer métodos continuos para una eliminación segura de datos que cumpla las directrices más rigurosas del RGPD en relación con la retención y el uso.

El departamento de TI también debería tomar la iniciativa implementando procesos sólidos para notificar violaciones de datos u otras formas de incumplimiento del RGPD. Teniendo en cuenta que esto puede implicar ponerse en contacto con los clientes (véase la página 11), el departamento de TI deberá contactar con todos los departamentos para asegurarse de que comprenden los requisitos de información del RGPD.

Al igual que antes, la duplicación de datos en tiempo real con fines de pruebas y preproducción se ve afectada por el RGPD, ya que tal vez no sea posible usar los datos de esta forma sin un consentimiento explícito.

“A menudo las empresas más pequeñas controlan mejor lo que hacen exactamente, lo que les ayuda a encontrar la base desde la que empezar a realizar cambios. Esto es una ventaja.

Pero el cumplimiento al que tienen que enfrentarse ahora es una carga de trabajo adicional con la que probablemente no contaban. No están acostumbradas a tener ese nivel de control.

Creo que muchas empresas están bastante sorprendidas de que necesiten documentar y aprobar toda esta información, para que luego puedan demostrar que están haciendo lo que dicen.”

Lograr el cumplimiento correcto del RGPD puede ser una tarea realmente laboriosa. ¿Es adecuada la forma en que una empresa desarrolla sus actividades? ¿Debe seguir haciéndolo así? Todo esto puede significar tener que ajustar o incluso cambiar algunos procesos empresariales importantes. En ocasiones resulta mejor rediseñarlos y encontrar una forma mejor de hacerlos.

David Clarke

(FBCS CITP), Fundador de GDPR Technology Group

PREGUNTAS Y RESPUESTAS SOBRE EL RGPD

A continuación, se incluyen respuestas a preguntas frecuentes planteadas por empresas que están implementando el RGPD.

¿Es necesario que mi empresa obtenga la "certificación del RGPD"?	No. La redacción del RGPD no especifica o exige un sistema de certificación concreto, pero fomenta la certificación voluntaria a través de organismos u organizaciones de la industria que cumplan la norma EN-ISO/IEC 17065/2012 y que tengan la autorización de las autoridades de control relevantes.	Aunque se fomenta obtener la certificación del RGPD para ofrecer garantías en relación con las medidas de seguridad organizativas y técnicas, entre otras cosas, hacerlo es especialmente importante para terceros que procesan datos en nombre de otros (los denominados encargados de tratamiento, véase la página 8).
Mi empresa vende o proporciona servicios directamente a empresas, no a personas. ¿Me afecta el RGPD?	Probablemente. Por ejemplo, si envías un correo electrónico a una persona en una empresa para organizar una venta, al conocer su dirección de correo estás recopilando datos identificativos sobre ella para ejercer una actividad económica.	Resulta imposible imaginar una situación comercial en la que tales datos no se generen o recopilen, incluso sin saberlo. Además, el RGPD también afecta a tu empresa internamente. Indica, por ejemplo, la forma en que gestionas los datos del personal y las nóminas (véase la página 21).
Dirijo un negocio muy pequeño del que solo yo formo parte. ¿Me afecta el RGPD?	Sí. El RGPD afecta a cualquier persona o entidad implicada en una actividad económica y que procesa datos personales, incluso en el caso de organizaciones como	asociaciones, entidades benéficas o clubs/sociedades. No importa si dicha entidad tiene reconocimiento legal.
¿Deberá mi empresa someterse a auditorías o inspecciones del RGPD?	El RGPD no incluye requisitos de auditorías o inspecciones gubernamentales periódicas, pero las autoridades de control tienen derecho a lleva a cabo auditorías como parte de sus competencias de investigación. Sin embargo, eso no quiere decir que las auditorías o inspecciones voluntarias no sean una muy buena idea o incluso un requisito de facto para el cumplimiento del RGPD. En el caso de terceros que proporcionan servicios de tratamiento de datos a otros, la situación es algo más complicada. También deben permitir y participar en las auditorías, incluyendo inspecciones, que exija la empresa que los contrata.	Sin embargo, el RGPD presenta nuevos requisitos importantes y complejos para el mantenimiento de registros para todas las empresas. No basta simplemente con cumplir el RGPD. Las empresas deben poder demostrar que lo están haciendo. Además de la documentación en la que figuran los procesos y otros datos, esto puede incluir tener que demostrar que se ha implementado la formación correcta. Ten en cuenta que existe la posibilidad de que los gobiernos implementen procesos de auditoría formales periódicos cuando apliquen el RGPD en su legislación nacional.

¿Por qué se introduce el RGPD si ya tenemos leyes de protección de datos?	Se trata principalmente de actualizar las leyes de protección de datos en función de las tecnologías modernas y también de las expectativas actuales de la gente. La normativa también mejora considerablemente los derechos de los interesados. El ámbito de la protección de datos se amplía en gran medida. Por ejemplo, ahora se incluyen cuestiones como los datos de ubicación que puede recopilar un smartphone, o bien los datos genéticos y biométricos, pero también incluye tipos de datos nuevos y adicionales que podrían	usarse tipos de datos nuevos y adicionales que podrían usarse para identificar a una persona, como su trasfondo cultural o social. Además, el RGPD no se centra únicamente en cómo las empresas deben proteger los datos. También otorga a las personas nuevos e importantes derechos sobre los datos que la empresa posee de ellos, lo que también podría implicar nuevas tareas y preparación para tu empresa. Las personas también disponen de nuevos derechos para entablar demandas colectivas en caso de una violación de datos.
¿Están los productos de Sage preparados para el RGPD?	Sage está trabajando para garantizar que todos sus productos activos estén preparados para el RGPD. En línea con las recomendaciones gubernamentales de distintos países, Sage recomienda a los usuarios asegurarse siempre de que utilizan las versiones de software más recientes.	En concreto, para ayudar a las organizaciones a cumplir sus obligaciones relacionadas con el RGPD, Sage puede continuar proporcionando mejoras y, por tanto, se aconseja a los clientes consultar periódicamente la versión más reciente disponible e instalar actualizaciones según sea necesario. Los clientes que ejecutan productos en la nube, como los de Sage Business Cloud, se beneficiarán continuamente de las versiones de software más recientes.
Ya cumplo la actual LOPD. ¿Tengo que hacer algo?	Probablemente. El RGPD sustituye todas las legislaciones nacionales existentes acerca de la protección de datos para los Estados miembros de la UE.	Cabe destacar que, como el RGPD es una normativa europea, siempre tiene prioridad sobre la legislación propia de un país. Por otro lado, es posible que el proyecto de ley de protección de datos incluya cuestiones que aún no forman parte del RGPD.

¿Aún tengo que cumplir con las solicitudes de consulta de datos de un sujeto?	Sí, aunque ya no puedes cobrar una tarifa en la mayoría de los casos y ahora debes responder en un mes.	Además, ya no puedes exigir exclusivamente solicitudes por escrito (es decir, solicitudes por correo postal) y también debes responder a las solicitudes online, como por correo electrónico.
¿Cuánto le va a costar el RGPD a mi empresa?	Es probable que los gastos para una empresa media incluyan algunos, si no todos los siguientes: • Auditorías de todos los procesos en todos los departamentos (lo idóneo es que las realice una persona o empresa con la cualificación necesaria) • Modificaciones como el reciclaje del personal y las adaptaciones de tecnologías de la información • Posible designación y formación de un Delegado de Protección de Datos (DPD; véase más abajo)	• Configuración y mantenimiento de procesos de documentación continuos que demuestren el cumplimiento del RGPD • Costes de certificación voluntaria, especialmente si tu negocio procesa datos en nombre de otras empresas Solo debes usar organismos de certificación que cumplan la norma EN-ISO/IEC 17065/2012 y que tengan la autorización de las autoridades de control relevantes.
Mi empresa no está ubicada en la UE. ¿Cómo se ve afectada, en caso de estarlo?	El RGPD afecta a cualquier empresa, sin importar su ubicación, que procese los datos de personas en la UE (véase Expansión del ámbito y el área geográfica en la página 10). De hecho, si ofreces bienes o servicios a personas en la UE o si monitorizas su comportamiento, probablemente deberás emplear a un representante en la UE para que gestione las consultas del RGPD. Además, debes notificar por escrito a la autoridad supervisora la identidad de esta persona. Muchos terceros ya están especializados en atender esta necesidad de representación y es posible encontrarlos en Internet.	Como mínimo, deberías investigar si este requisito se aplica a tu empresa. Antes de la entrada en vigor del RGPD, actualmente es difícil predecir las consecuencias para las empresas ubicadas fuera de la UE que incumplen el RGPD, pero podrían incluir la prohibición de realizar transacciones comerciales dentro de la UE hasta que se demuestre el cumplimiento, lo que podría llevar algún tiempo. Esto podría afectar no solo a las ventas, sino también a los proveedores y, por tanto, su efecto podría ser devastador.

#IProtectData

Comparte el mensaje. Comparte la responsabilidad.

En Sage comprendemos que nuestros productos y servicios pueden formar parte de los controles y procesos que las empresas deben establecer para cumplir sus propias obligaciones en relación con el RGPD. Vamos a respaldar este esfuerzo revisando todos nuestros productos y documentación complementaria, o publicando actualizaciones a las versiones compatibles más recientes para los clientes. Esto incluye desarrollar más avances tecnológicos con nuestros productos para garantizar que nos mantenemos a la vanguardia de la portabilidad de datos, el mantenimiento de registros y el derecho de supresión a medida que se desarrolla el RGPD.

Para ver nuevos recursos sobre el RGPD y lo que Sage está haciendo para garantizar que sus productos estén preparados para esta nueva normativa :

visita: **www.sage.com/es-es/rgpd**

Todos los derechos reservados. Sage, los logotipos de Sage y los nombres de los productos y servicios de Sage aquí mencionados son marcas comerciales de The Sage Group plc o de sus licenciantes. Todas las demás marcas comerciales son propiedad de sus respectivos dueños.