Reglamento General de Protección de Datos (RGPD):

Guía rápida de Sage para empresas

Índice

Introducción

El Reglamento General de Protección de Datos (RGPD) constituye el nuevo marco jurídico que entrará en vigor el 25 de mayo de 2018 en la Unión Europea (UE). Los reglamentos de la UE son de aplicabilidad directa en todos sus Estados miembros, por lo que el RGPD tendrá prioridad sobre las legislaciones nacionales.

El objetivo del RGPD es la protección de los datos personales, es decir, los relativos a personas físicas. De hecho, el RGPD es una de las mayores reestructuraciones de cómo debería ser el tratamiento de los datos personales y puede llegar a afectar no solo a las empresas, sino a cualquier persona, entidad, autoridad pública, servicio u otro organismo que procese datos personales de quienes residan en la UE. Ahí se incluyen proveedores y terceras empresas a los que se encargue el tratamiento de datos personales.

Su ámbito de aplicación es sorprendentemente amplio: todos los Estados miembros de la Unión Europea, así como el Reino Unido tras su salida (Brexit) de la UE en 2019, ya que el GDPR también se incorporará a la legislación británica. A diferencia de las normas de protección de los datos personales recogidas en la directiva 95/46/CE, el RGPD también afecta a las empresas de fuera de la UE que ofrezcan bienes o servicios a personas de la UE o que controlen su comportamiento dentro de la UE. Por ejemplo, afecta directamente a las empresas estadounidenses que alojen sitios web accesibles para las personas de la UE.

El RGPD tiene implicaciones enormes para todos los departamentos de muchas compañías de todo el mundo. En algunos casos tendrán que contratar o designar un delegado de protección de datos, por ejemplo. Casi todas deberán aplicar procedimientos y garantías adicionales. Se recomienda encarecidamente que alguien con la formación adecuada lleve a cabo una auditoría y que, ante la posibilidad de incurrir en una sanción 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), se considere imprescindible conocer el RGPD.

El presente documento pretende ser una guía concisa y simplificada para empresas. Puede encontrarse más información a través de las autoridades de control, como la Agencia Española de Protección de Datos en el caso de España. Asimismo, conviene leer el Aviso legal de Sage que figura al final de esta guía.

Infografía:

El RGPD de un vistazo

Reglamento General de Protección de Datos (RGPD)

Consentimiento

Debe ser una declaración u otra acción afirmativa clara. No se puede dar por supuesto ni siquiera usar casillas ya marcadas en una web.

Derechos del individuo

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

Delegado de protección de datos

Puede 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.

Conceptos básicos

El RGPD establece los requisitos mínimos que debe cumplir el tratamiento de todos los datos personales. Por datos personales se entiende toda información (tales como el aspecto físico o incluso datos biométricos) sobre una persona física identificada o identificable.

La mayoría de las empresas recogen datos personales en cuanto interactúan con una persona, a veces incluso sin darse cuenta. Por ejemplo, se considera recogida de datos personales desde algo tan elemental como la «cookie» que identifica a un usuario de un sitio web hasta algo tan detallado como la ficha de un contacto en una base de datos de gestión de relaciones con clientes (o CRM), o incluso más. Aunque los datos personales se recojan o traten únicamente en beneficio de esa persona, siguen quedando protegidos dentro del ámbito del RGPD.

Igual que la directiva 95/46/CE, el RGPD reafirma tres conjuntos básicos de normas relativas a los datos personales: principios de la protección de datos, tratamiento lícito y limitaciones a las transferencias internacionales. La mayoría de las empresas deberían conocerlas ya, y muchas personas también las tendrán presentes. Estos tres conjuntos de normas se describen con más detalle en el presente documento y bien merecen su lectura aunque solo sea para refrescar los conocimientos existentes.

Aun así, el RGPD introduce nuevos requisitos de gran importancia.

El RGPD en resumen

Las siguientes son las principales áreas del RGPD, en especial con respecto a la directiva 95/46/CE de protección de datos de carácter personal.

Los derechos del individuo y cómo informar sobre ellos

La norma vigente actualmente para la protección de datos en la UE (directiva 95/46/CE) otorga a las personas físicas derechos sobre sus datos personales y describe la información que deben recibir de las empresas, incluidos los fines que van a darles a esos datos. En muchos casos, dicha comunicación consiste en declaraciones de privacidad o en notificaciones proporcionadas en un sitio web.

El RGPD amplía la protección considerablemente, ya que da más derechos que, una vez más, deben comunicarse a los interesados. En concreto, debe informárseles de que tienen los siguientes derechos (entre otros):

1. A la queja ante las autoridades de control, como la Agencia Española de Protección de Datos
2. A la retirada del consentimiento al tratamiento de sus datos personales (véase más abajo)
3. Al acceso a sus datos personales, así como a su rectificación o supresión («el derecho al olvido») por parte de la empresa y por terceros que hayan tenido acceso a ellos
4. Al conocimiento de la existencia de cualquier tratamiento automatizado de los datos personales (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 informado de cuánto tiempo se conservarán los datos personales
7. A conocer los datos de contacto de los delegados de protección de datos designados (véase más abajo)

Además, las personas físicas tienen el derecho a que, en su nombre, organizaciones sin ánimo de lucro ejerzan derechos y presenten reclamaciones (a la manera de las demandas colectivas del derecho estadounidense).

Consentimiento

Aunque la legislación de la UE siempre ha requerido que el consentimiento de las personas para la recogida de sus datos sea libre, específico e informado, el RGPD exige que sea confirmado mediante una declaración u otra acción afirmativa clara. Es decir, las casillas ya marcadas en las páginas web, el silencio o la inacción del interesado después de leer una declaración de privacidad no constituyen consentimiento.

Además, el consentimiento no puede ser genérico, por lo que un consentimiento otorgado por una persona a una empresa para cierta gestión no puede servir para otros tipos de tratamiento de datos personales. Para diferentes operaciones de tratamiento se necesitan consentimientos independientes.

Por último, no solo es necesario informar a las personas de que tienen derecho a retirar su consentimiento en cualquier momento, sino que debe ser tan fácil retirarlo como darlo.

Los consentimientos ya otorgados por las personas deben revisarse para verificar que cumplen los requisitos del RGPD. En caso de conflictos o ambigüedades, las empresas deberán establecer una nueva base lícita para el tratamiento de los datos personales (por ejemplo, si es necesario para la realización de un contrato), obtener un nuevo consentimiento o cesar en el tratamiento de dichos datos.

Derecho a la circulación o transferencia (portabilidad) de los datos personales

Las personas tienen ahora el derecho a mover, copiar o transferir sus datos personales de un lugar a otro, incluso a un competidor. Por ejemplo, si un usuario ha generado una lista de reproducción en un servicio de música y cambia de proveedor, puede llevársela consigo. Así pues, los datos personales deben tener un formato estructurado, de uso común y lectura mecánica para que sean fáciles de utilizar y compartir.

Es probable que la exigencia de que los datos sean realmente portátiles y fáciles de usar para otros obligue a realizar ajustes importantes en los sistemas informáticos, con los costes consiguientes.

Extensión del ámbito de aplicación

En pocas palabras, el RGPD hace responsable de las violaciones de la seguridad de los datos personales no solo a la empresa que los recoge, sino también a cualquier tercero que los procese en nombre de ella, ya sea otra empresa, un organismo o una persona física. No obstante, eso no implica que una empresa puede limitarse a transmitir los datos personales a un tercero y desentenderse. La empresa debe asegurarse de que el tercero también cumpla el RGPD.

Además, el posible ámbito territorial de aplicación se extiende más allá de la UE a cualquier empresa —o, de nuevo, a cualquier tercero que procese datos personales en su nombre— que ofrezca bienes o servicios a personas físicas que residan en la UE o que controle el comportamiento de ellas. Cabe destacar que es irrelevante si se paga por los bienes o servicios; así pues, la aplicación del RGPD también afecta a instituciones benéficas y a ONG´s.

Dado que la UE es un socio comercial de la mayoría de los países, la ampliación del ámbito de aplicación del RGPD tiene implicaciones para muchas empresas de todo el mundo y, en la práctica, les obligará a cumplirlo si desean operar en los Estados miembros de la UE, ya sea directamente o dando servicio a otros.

Prueba de cumplimiento

No basta con simplemente cumplir el RGPD. Las empresas deben demostrar que lo hacen de acuerdo con el requisito de «responsabilidad proactiva», que implica cumplir algunas obligaciones bastante onerosas de llevanza de registros. En concreto, deben mantenerse registros que detallen las actividades de tratamiento*, las peticiones de acceso de los interesados, las violaciones de seguridad, la forma de obtención de los consentimientos y las evaluaciones de impacto relativas a la protección de datos (véase más abajo).

Una vez más, este requisito también afecta a los terceros que procesen datos personales en nombre de una empresa, si bien la especificación no es tan detallada.

** Es aplicable a empresas que empleen a más de 250 personas, o a las que empleen a menos pero en las que el tratamiento probablemente entrañe un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos, tales como información sobre la salud, la religión o la orientación sexual.*

Privacidad de principio a fin

Durante toda la vida útil de los datos personales —desde su recopilación hasta el cese definitivo de su uso— deben tomarse medidas técnicas y organizativas acordes a las expectativas de privacidad del interesado. Es lo que se denomina «protección de datos desde el diseño» e implica que las consideraciones de privacidad deben estar incorporadas en todos los aspectos de ese tratamiento desde el diseño.

Asimismo, solo deberían tratarse los datos personales estrictamente necesarios para el fin buscado —a lo que se denomina «protección de datos por defecto»—.

En realidad, la aplicación de la protección de datos desde el diseño y por defecto implicará la formación continua, la realización de auditorías periódicas, la minimización de los datos recogidos, el acceso a los datos personales solo cuando sea necesario y la aplicación de las adecuadas medidas de seguridad técnicas y organizativas, tales como la seudonimización o el cifrado.

Comunicación obligatoria de las violaciones de la seguridad

En caso de producirse violaciones del RGPD, las empresas que recogen datos personales deben informar a las autoridades de control —como la AEPD en España— en el plazo de 72 horas desde su conocimiento. Las terceras empresas que procesen los datos personales en nombre de otras empresas deben avisarlas sin dilación indebida.

Si la violación entraña un alto riesgo para los interesados, las empresas deben notificárselo a ellos sin dilación indebida.

Delegado de protección de datos (DPD)

Según el RGPD, las empresas y los terceros que procesen datos personales en su nombre deberán designar un delegado de protección de datos (DPD) siempre que: (i) sean un organismo público; (ii) las actividades principales de la empresa o el tercero consistan en la observación de interesados a gran escala; o (iii) sus actividades principales consistan en el tratamiento a gran escala de categorías especiales de datos personales, tales como datos relativos a condenas o infracciones penales. El DPD debe tener conocimientos especializados de la legislación de protección de datos, aunque no es imprescindible que sea empleado directo, sino que puede desempeñar esta función en el marco de un contrato de servicios. Los datos de contacto del DPD deben comunicarse a la autoridad de control, como la AEPD en España.

Sanciones

Las sanciones por el incumplimiento del RGPD son duras y podrían ascender al 4 % del volumen de negocio anual en todo el mundo o a 20 millones de euros, la cuantía que sea mayor. La sanción puede imponerse aunque no haya pérdida en sí de los datos. Cabe destacar que no existen exclusiones ni excepciones para las pequeñas empresas. Además, las personas físicas tienen la posibilidad de presentar una demanda colectiva solicitando una investigación formal si una empresa no cumple el RGPD.

Brexit

Tras las elecciones celebradas en el Reino Unido en 2017, el Partido Conservador vuelve a gobernar. Durante los cinco años de su mandato, en concreto en 2019, el Reino Unido abandonará la Unión Europea. Como en todos los Estados miembros de la UE, el RGPD se aplicará en el Reino Unido hasta ese momento. Sin embargo, en el anuncio de nueva legislación tras las elecciones, se señalaba que las nuevas leyes de protección de datos:

> *«... pondrán en práctica el Reglamento General de Protección de Datos y la nueva directiva que se aplica al tratamiento de datos policiales, cumpliendo nuestras obligaciones mientras sigamos siendo un Estado miembro de la UE y ayudando a poner al Reino Unido en la mejor situación para mantener la capacidad de compartir datos con otros Estados miembros de la UE y con otros países tras nuestra salida de la UE.»*
>
> *Fuente: Discurso de la Reina, junio de 2017*

Por lo tanto, es posible, pero no seguro, que la Comisión Europea considere que el Reino Unido después del Brexit proporciona una protección «adecuada», en cuyo caso no se vería afectado por posibles problemas, como la prohibición de la transferencia de datos personales. Próximamente iremos informando de las decisiones que se vayan tomando.

La nueva legislación del Reino Unido sustituye a su ley de protección de datos de 1998, que se basaba en la directiva 95/46/CE.

Principios básicos del RGPD

Además de los nuevos requisitos detallados más arriba y al igual que sucede con la directiva 95/46/CE, el RGPD reafirma tres conjuntos básicos de normas relativas a los datos personales. En términos sencillos, pueden describirse como sigue:

- ***Principios de la protección de datos:*** el tratamiento de los datos personales debe ser lícito, leal y claro para el interesado. Deben recogerse para fines específicos, explícitos y legítimos, y no pueden tratarse de una forma que sea incompatible con ellos. Los datos recogidos deben ser adecuados, pertinentes y limitados a lo necesario. Deben ser exactos y mantenerse actualizados, y deben tomarse todas las medidas razonables para garantizar que los datos personales que sean inexactos se rectifiquen o supriman sin demora. Los datos personales deben almacenarse de un modo que identifique al interesado solo el tiempo necesario, y deben tratarse de manera que se garantice su seguridad, incluida la protección frente a pérdida, destrucción o daños, así como el acceso ilícito o no autorizado.
- ***Tratamiento lícito:*** solo es lícito el tratamiento de datos personales si se cumple al menos una de las siguientes condiciones. El interesado ha dado su consentimiento para uno o más fines específicos; es necesario para un contrato en el que interviene, o pronto intervendrá, el interesado; debe cumplirse una obligación legal (por ejemplo, declaración de impuestos de una empresa); existe una misión realizada en el interés público o en el ejercicio de poderes públicos; es necesario para proteger intereses legítimos (incluso de un tercero), salvo que prevalezcan los intereses, derechos fundamentales y libertades del interesado.
- ***Transferencias internacionales:*** el RGPD mantiene la prohibición general de enviar datos personales fuera del Espacio Económico Europeo a un país que no ofrezca una protección adecuada. En el momento de redactar este documento, los países que la Comisión Europea considera que ofrecen una protección adecuada son: entidades estadounidenses que se hayan autocertificado en el Escudo de la privacidad UE-EE. UU. (nota: esto no implica que se considere que Estados Unidos como país proporciona una protección adecuada), Andorra, Argentina, Canadá (solo PIPEDA), Islas Feroe, Guernsey, Israel, Isla de Man, Jersey, Nueva Zelanda, Suiza y Uruguay. Si no existe decisión sobre la adecuación, solo pueden transferirse datos en circunstancias limitadas, tales como, sobre la base del consentimiento, el uso de cláusulas contractuales tipo publicadas por la Comisión Europea o, en el caso de transferencias interempresariales, el uso de normas corporativas vinculantes.

Cómo puedes empezar a prepararte

- Para más información, visita la zona del sitio web de la AEPD dedicada al nuevo Reglamento General de Protección de Datos, donde podrás encontrar varias guías e información general. En concreto, consulta la publicación de la AEPD, «Guía del Reglamento General de Protección de Datos para responsables del tratamiento».
- Revisa tus sistemas de captura y tratamiento de datos personales para asegurarte de que sean conformes con el RGPD. Deberías pensar en realizar una auditoría de RGPD desde los puntos de vista legal y tecnológico, entre otros.
- Asegúrate de que tus empleados y proveedores conozcan el RGPD y organiza cursos para que estén preparados. Recuerda que el RGPD también te hace responsable del tratamiento de datos personales que terceros hagan para ti.
- Asesórate para comprender mejor las implicaciones del RGPD para tus actividades.

Para más información, visita: Sage.com/GDPR

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 este sitio web 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 esta información.