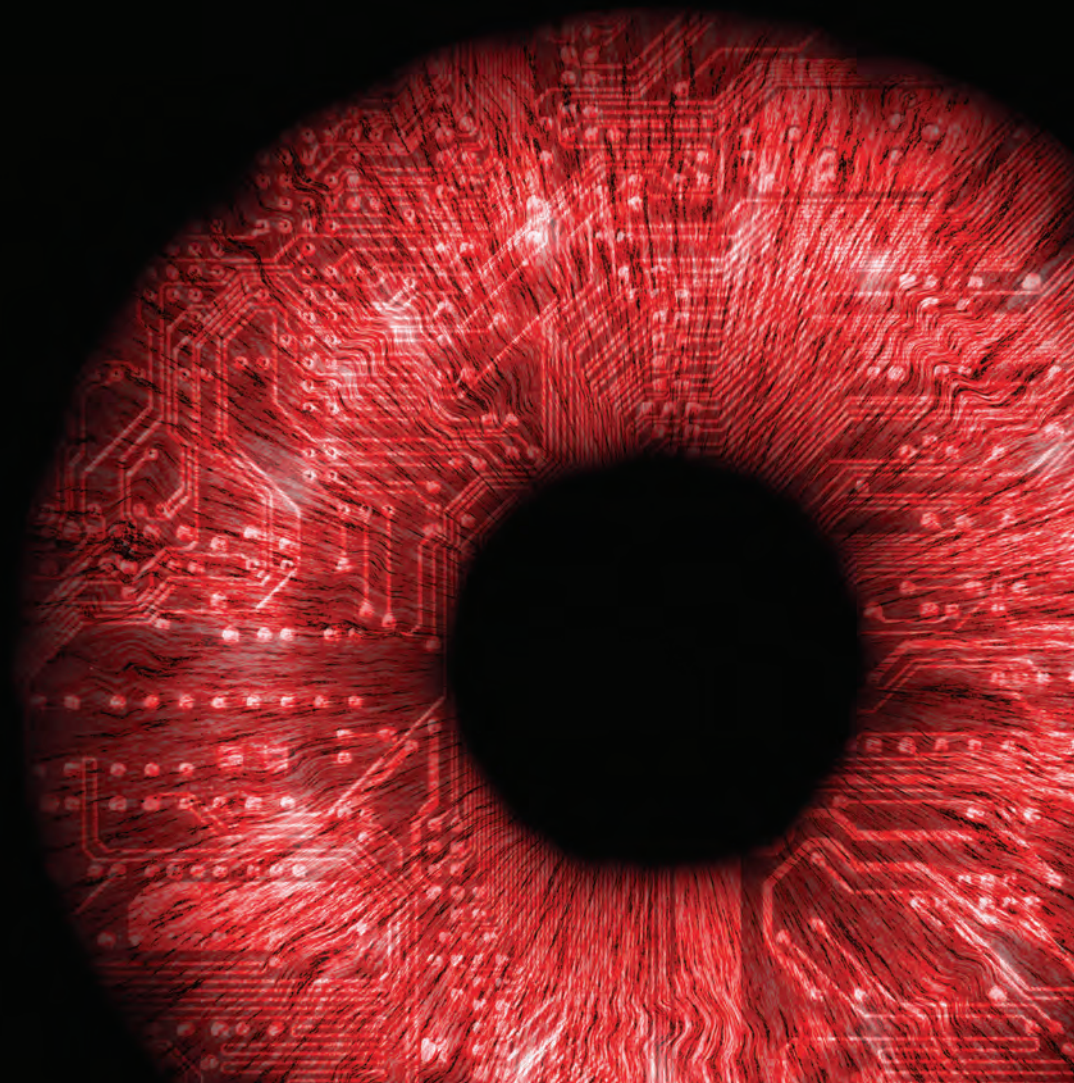
HISCOX

¿ESTÁ TU NEGOCIO PREPARADO PARA EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS?



Introducción

Antes del próximo 25 de mayo las compañías deben adaptar su política de gestión de la información personal de sus clientes al nuevo Reglamento General de Protección de Datos (RGPD).

El primer paso es comprender quién se verá afectado por este nuevo reglamento. El RGPD se aplicará a cualquier empresa que ofrezca bienes o servicios que gestionen datos de personas que habiten en los estados miembros de la Unión Europea. Este aspecto es importante, ya que no estamos hablando solo de entidades con sede en estos países, sino que el reglamento afecta a cualquier empresa, esté donde esté, cuyos clientes sean residentes en esta área geográfica.

Tenemos un compromiso con el tejido empresarial asegurando a más de 300.000 profesionales y compañías en todo el mundo que nos empuja a llevar nuestra colaboración con ellos siempre un paso más allá. Por ello, nuestros especialistas en servicios para empresas y ciberseguridad han preparado esta guía donde resolvemos las siguientes cuestiones:

1. ¿Qué es el nuevo Reglamento General de Protección de Datos?
2. ¿Qué debo hacer para cumplir con el RGPD?
3. ¿Qué pasa si vulnero la protección de datos de mis clientes con el nuevo reglamento ?
4. ¿Cuáles serán las consecuencias de no adaptar mi negocio?
5. ¿Dónde puedo obtener más información u apoyo adicional?

1. ¿Qué es el nuevo Reglamento General de Protección de Datos?

El Reglamento General de Protección de Datos (GDPR) (Reglamento UE 2016/679) es un marco normativo por el cual el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea, se proponen fortalecer y unificar la protección de datos, y su libre circulación, para todas las personas dentro de la Unión Europea. Esta nueva legislación otorgaba un periodo de adaptación de dos años, que finaliza en mayo de este año.

La respuesta de la Unión Europea al nuevo paradigma de la privacidad

La normativa tiene como objetivo salvaguardar los datos personales de los ciudadanos de la Unión Europea que manejan instituciones públicas, empresas y organizaciones de todo el mundo. Así, ante el nuevo paradigma de la ciberseguridad, millones de datos -nombres, direcciones, datos personales, e incluso identificadores online (por ejemplo, una dirección IP)- gozarán de una mayor protección a partir del 25 de mayo de 2018.

Soy una empresa pequeña… ¿tengo que cumplir el reglamento?

Sí. Tengas el tamaño que tengas y pertenezcas al sector que pertenezcas, toda compañía o institución que maneje información sobre ciudadanos de la UE estará bajo el alcance de este nuevo reglamento. Existen algunas singularidades que tienen en cuenta los menores recursos de las PYMES, como por ejemplo, no obligándolas a designar un delegado de protección de datos (DPD) de la compañía. Aun así, el nuevo reglamento es tan riguroso, que incluso si una PYME se encuentra dentro de estas excepciones pero es proveedor de una compañía a la que sí se le exige el mayor de los niveles de seguridad, esta PYME podría estar obligada a cumplir los mayores estándares posibles también.

Una vez más, las grandes corporaciones están llamadas a liderar el cambio y abrir el camino para la adaptación del tejido empresarial. En este sentido, ya son muchas de ellas las que están preparando la llegada del RGPD: blindando los datos de sus clientes y exigiendo a sus proveedores y colaboradores, por contrato, cumplir con ciertos requisitos de seguridad.

Oportunidad de negocio

El nuevo marco podría convertirse en una ventaja competitiva para muchas empresas cuando se trate optar a un nuevo negocio. Las empresas deberían aprovechar el GDPR como catalizador para transformar sus compañías en negocios centrados en el cliente, y utilizando el nuevo reglamento como base para una relación auténtica y transparente con sus clientes.

2. ¿Qué debo hacer para cumplir con el RGPD?

Hay una serie de sencillos pasos a tener en cuenta para asegurarnos de que estamos preparados para cumplir con los requisitos antes del 25 de mayo de 2018.

¿Qué datos tengo, de dónde provienen y por donde circulan?

En primer lugar, es importante comprender y controlar qué datos personales manejo en mi negocio, cómo los conseguí, cómo se almacenan, cómo se usan y por dónde pueden circular. La UE define 'datos personales' como: 'cualquier información de un individuo, ya esté relacionada con su vida privada, profesional o pública'. Puede ser cualquier cosa, desde un nombre, una foto, una dirección de correo electrónico, datos bancarios, sus publicaciones en redes sociales, su información médica o la dirección IP de su ordenador. Se amplía así el concepto dato personal respecto al marco normativo anterior, al incluirse conceptos como, ID de dispositivos, datos de ubicación y datos genéticos y biométricos.

La Figura del responsable de tratamiento y del encargado de tratamiento: responsabilidades

Existen dos tipos de entidades que pueden operar con datos personales. Por un lado, está el denominado responsable de tratamiento, quien posee los datos, y determina sus fines, uso y circulación. Por otro lado, el encargado de tratamiento, quien puede procesar datos personales en nombre del responsable de tratamiento. La obligación de proteger los datos ahora es compartida entre el responsable y el encargado de tratamiento y ambos están regidos por el RGPD. Además, los encargados de tratamiento estarán sujetos a sanciones cuando no cumplan con las obligaciones contractuales o actúen fuera de las instrucciones del controlador.

6 principios para las empresas respecto a cómo deben ser los datos personales que gestionan:

1. Transparentes, justos y legalmente procesados.
2. Procesados para un propósito específico.
3. Adecuados y relevantes para el propósito para el que se están procesando.
4. Precisos (eliminándolos y corrigiéndolos con mayor regularidad).
5. No deben ser conservados más tiempo del necesario y para el propósito para el que se está procesando.
6. Guardarlos de forma segura.

¿Tenemos consentimiento para recoger y operar con estos datos?

El GDRP hará mucho más complicado conseguir el consentimiento para para procesar los datos personales de un sujeto (por ejemplo, para fines comerciales). La definición de consentimiento se ha ajustado de manera que debe ser 'inequívoca' cuando se produzca, es decir, que el individuo de manera activa haya marcado una casilla o seleccionado la opción de consentimiento. Además se aplica con carácter retroactivo, por lo que deberemos conseguir el permiso inequívoco también de los datos personales que tenemos ya almacenados.

Las solicitudes de consentimiento deberán presentarse de manera individual, con su propio espacio, de modo que ya no podrán estar incluidas, ni ocultas, dentro de otras políticas o letras pequeñas. Así, además de conseguir ese consentimiento, deberemos poder demostrar, llegado el caso, cuál fue el proceso a través del cual los conseguimos. Las casillas previamente marcadas o la no respuesta como respuesta positiva, ya no serán válidas, solo se dará por bueno el proceso de obtención si hemos conseguido el consentimiento de manera activa por parte del sujeto.

Ante esta nueva exigencia las compañías deben preguntarse, ¿cómo obtengo los consentimientos ahora?, y ¿qué cambios necesitaré realizar en los procesos para asegurarme que podré demostrar dónde, cuándo y cómo las personas me dieron su consentimiento para procesar sus datos?

La protección de datos concebida desde el diseño

Ahora la protección de los datos debe ser considerada e integrada en cualquier sistema o proceso desde su propia concepción, tanto en términos de forma en los que se diseñen, como en las políticas y procedimientos establecidos para dictar cómo las personas deberían usarlos.

Una solución en este campo sería el uso del cifrado. Este elemento ofrece un perfil de seguridad más alto, y además puede reducir la multa a la que estamos expuestos, así como la probabilidad de que seamos sancionados en caso de que se produjera una violación de datos.

Derecho de acceso a los datos

Las personas aumentan sus derechos en lo que respecta a la forma en que se protegen sus datos personales. Las empresas deben asegurarse de que existen procesos y plantillas adecuadas para que cualquier sujeto que quiera ejercer su derecho sea respondido en un plazo máximo de un mes.

¿De qué derechos hablamos?

- Tener fácil acceso a todos sus datos personales almacenados.
- Derecho a rectificación de datos inexactos.
- Negar el procesamiento de sus datos en ciertas circunstancias, como por ejemplo si se trata de su comercialización.
- Derecho a trasladar sus datos de un servicio a otro.
- Exportar los datos en un formato que se pueda ser usado en otros entorno de TI.
- Eliminar por completo, en ciertas circunstancias, todos sus datos.
- El consentimiento debe ser claro, dado en libertad, específico, informado y sin ambigüedades. Además, adicionalmente, este consentimiento debería ser desglosado, detallado, definido, documentado y de fácil rescisión.
- Información clara sobre el procesamiento.
- Derecho a notificación si los datos se ven comprometidos.
- Requisitos de seguridad más estrictos para ser transferidos fuera de la UE.

¿Sabemos qué constituye una violación de datos personales?

Debemos asegurarnos de que todas las personas que forman parte de nuestra compañía comprendan qué constituye una violación de datos, así como establecer un proceso para localizar eslabones o procesos internos más débiles. Este trabajo de sensibilización y formación será vital para estar preparados ante la inminente entrada del GDPR.

Pero además de capacitar y dar las herramientas necesarias a todo el equipo, también debemos desarrollar y fomentar una cultura en la que los empleados se sientan cómodos y den aviso cuando cometan un error inocente, la causa principal de la gran mayoría de las violaciones de datos.

Revisar nuestros términos y condiciones, y los contratos con proveedores

En la adaptación de nuestro negocio al GDRP debemos incluir también a aquellos proveedores que procesen datos personales en nuestro nombre o coordinados con nosotros, para asegurarnos de que existe la protección adecuada y exigida en el nuevo marco reglamentario. Así, podemos solicitarles que completen un formulario para evaluar qué medidas y estrategia de ciberseguridad tienen implementadas, y a partir de ahí poder revisarlas para ver si son suficientes o realizar una auditoría físicamente en el lugar.

Además, cuando nuestros proveedores procesen datos personales en nuestro nombre tendremos la obligación de actualizar nuestros contratos con ellos para incluir una serie de cláusulas obligatorias que se pueden encontrar en el Artículo 28 de la GDPR. Así, aseguraremos que el proveedor esté por contrato obligado a proporcionar estándares de protección de datos compatibles con el GDRP.

Evidentemente, se pude producir el caso inverso, que seamos nosotros los proveedores que procesan datos personales para otras compañías, así, seremos nosotros a los que se le apliquen estos criterios. Estar preparado nos ayudará ante posibles negociaciones de nuevos contratos y nos dará una ventaja competitiva.

Revisar nuestro aviso de privacidad

Ante los nuevos requisitos es probable que nuestra política de privacidad sea más extensa. Tendremos que entrar en más detalles, y además deberá ser comprensible y accesible. El contenido variará si los datos personales recogidos son para nuestro uso o los estamos almacenando para un tercero. La información que debe ser suministrada incluirá:

- El fin para el que se están procesando los datos personales, así como la base legal para el procesamiento de los mismos (por ejemplo, consentimiento, intereses legítimos, requisitos contractuales, etc.).
- El destinatario o tipos de destinatarios entre los que podrían circular estos datos personales. El nombre y detalles de la entidad que controlará sus datos personales, y qué otras entidades que podrían hacer uso de sus datos personales.
- El período de retención de estos datos, o los criterios utilizados para determinar el período de retención.
- Información detallada de cada uno de los derechos de la persona que consiente (eliminación, portabilidad, rectificación, etc.).
- Cualquier otra información sobre el perfil de la entidad controladora que sea de su utilidad.

Además, aviso de privacidad deberá ser conciso, transparente, inteligible y de fácil acceso, y deberá estar escrito en un lenguaje claro y sencillo.

Caso práctico: Facebook recibió una multa de 1,2 millones de euros en España por infringir las leyes de privacidad. El regulador descubrió que Facebook no había informado a los usuarios cómo se usarían sus datos para campañas publicitarias. Se acusaba a Facebook de usar términos ‘genéricos’ y ‘poco claros’, y un política de privacidad de difícil acceso.

Datos de alto riesgo

Antes de comenzar el procesamiento de datos considerados de alto riesgo, será necesaria una evaluación documentada que identifique estos riesgos, para demostrar el cumplimiento con el GDPR. Aunque este requisito no especifica que datos podrían considerarse de alto riesgo, podría incluir información como capturas o procesamientos de datos confidenciales como detalles de cuentas bancarias o información de salud, que podría tener un impacto muy dañino para el individuo si estos datos quedaran expuestos.

¿Necesito designar a un delegado de protección de datos (DPD)?

Si bien la mayoría de las empresas con menos de 250 empleados estarán exentas, si sus actividades principales implican monitoreo o procesamiento a 'gran escala' de datos confidenciales (que incluyan datos que revelen origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación a sindicatos, o datos relacionados con la salud o la vida sexual), deberán designar un delegado de protección de datos independiente a la dirección de la compañía y al equipo que realice el procesamiento de datos. Así, las responsabilidades del delegado no podrán delegarse en un integrante del equipo de sistemas de la empresa.

Aunque hasta el momento no se ha definido completamente lo que constituye 'gran escala', algunos de ejemplos serían:

- Datos de pacientes para un hospital.
- Datos de personas que usan el servicio de transporte de pasajeros de una ciudad.
- Datos de clientes para una compañía de seguros o un banco.

Las entidades interesadas en obtener la acreditación para certificar a su DPD pueden solicitar información sobre cómo iniciar el proceso de acreditación a través de ENAC (Entidad nacional de acreditación).

Resumen: cinco claves para demostrar que hemos adaptado nuestro negocio:

- Implementar medidas técnicas y organizativas que garanticen y demuestren que nuestro negocio está adaptado: nuevas políticas, programas de formación y capacitación, auditorías y evaluaciones.
- Ofrecer documentación actualizada sobre los procesos que estamos adaptando.
- Si es el caso, designar un responsable de protección de datos.
- Implementar medidas que cumplan con los principios de diseño de protección de datos y protección de datos por defecto: minimización de datos y transparencia.
- Desarrollar evaluaciones de nuestros procesos de protección de datos.

3. ¿Qué pasa si vulnero la protección de datos de mis clientes con el nuevo reglamento en funcionamiento?

El GDPR define como 'violación de datos personales' una brecha de seguridad que permita la destrucción, pérdida, alteración, divulgación no autorizada o acceso a datos personales. Esto significa que una 'violación de datos personales' es más que simplemente ser pirateado o perder datos personales. Esto también se aplica a todos datos almacenados sea cual sea el proceso, así los datos en papel deben tratarse con el mismo nivel de cuidado.

Cuándo informar sobre una violación de datos

Las violaciones tendrán que ser notificadas a la Agencia Española de Protección de Datos si es 'probable que estén en riesgo los derechos y las libertades de las personas'. Los ejemplos proporcionados se ciñen a aquella información que pueda 'dar lugar a discriminación, daño a la reputación, pérdida financiera, pérdida de confidencialidad o cualquier otra desventaja económica o social significativa'.

Las violaciones de datos solo tendrán que notificarse a las personas afectadas cuando exista un 'alto riesgo' de los requisitos de información más estrictos.

¿Cuál es el plazo para informar de una infracción?

El aviso ante una infracción debe realizarse dentro de las primeras 72 horas de haberse producido, y el informe debe contener, como mínimo:

- La naturaleza de la violación de datos personales, incluidos, cuando sea posible, las categorías y el número aproximado de personas y de datos personales, el nombre y los datos de contacto del DPD (si nuestra organización tiene uno), o un un contacto donde poder ampliar la información.
- Una descripción de las consecuencias probables provocadas por esta violación de datos.
- Una descripción de las medidas propuestas o tomadas para gestionar la violación de datos personales y, en su caso, las medidas tomadas para minimizar cualquier posible efecto adverso.

Cómo evitar una violación de datos

Dadas la amplia definición de 'violación de datos personales' y 'datos personales', es casi inevitable que cualquier empresas caiga en una infracción menor (bastaría con enviar un correo electrónico a la persona equivocada), por lo que debemos pensar qué vamos a hacer cuando esto ocurra, especialmente teniendo en cuenta el estrictos plazo requerido para la notificación de la infracción.

Definir un plan de respuesta simple ante estos incidentes puede marcar una gran diferencia y minimizar el posible impacto negativo en nuestro negocio. Para ellos debemos tener claro:

- ¿A quién se debe informar internamente si se produce una violación?
- ¿Quién participa en la evaluación de las consecuencias de la violación?
- ¿Cuáles son nuestros sistemas y datos más sensibles, y a los que deberíamos darle prioridad en nuestros procesos de protección y restauración?

4. ¿Cuáles podrían ser las consecuencias de no adaptar mi negocio?

En primer lugar, hagamos nos esta pregutna en postivo, ¿qué conseguiré si cumplo con el GDPR?: garantizaré la mayor protección de los datos personales de mis clientes, protegiéndome a la vez de cualquier sanción o daño a mi reputación ganada con esfuerzo. Por tanto, cumplir con el nuevo reglamento beneficiará a mi negocio. Ahora bien, qué ocurre si no me adapto.

Multas por incumplimiento

El incumplimiento del GDPR, no solo si se produce un incidente, sino también si se comete un error administrativo y no se cumple con alguno de sus requisitos, podría dar lugar a una investigación regulatoria, que en sí misma requiere tiempo y esfuerzo por parte de una empresa, y nos expondrá a una multa.

En sus valores máximos, la multa podría llegar a suponer el 4% del volumen de negocio del último ejercicio o 20 millones de euros para las infracciones más graves, o hasta el 2% o 10 millones de euros para cuestiones de índole administrativo. Aunque sería muy sorprendente que una PYME llegue a ser multada en estos valores, la AEPD ha demostrado su voluntad de imponer sanciones financieras contra las PYME, aunque prestando siempre atención a su capacidad para continuar operando tras dicha penalización.

5. ¿Dónde puedo obtener más información u apoyo adicional?

Entidades públicas y privadas están proporcionando recursos a las empresas para asegurar que cumplen con los requisitos del GDPR antes del 25 de mayo de 2018. Aquí tenéis algunos de ellos:

La Agencia Española de Protección de Datos ha abierto un espacio dedicado a este asunto donde proporciona muchas actualizaciones con las últimas novedades, así como una Guía Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD.

Hiscox ofrece una solución de seguro de datos y ciberseguridad diseñada para proporcionar una respuesta rápida y experta en caso de una violación de datos personales, que puede, entre otras cosas, ayudar a una empresa a cumplir con los estrictos requisitos del GDPR.

Hiscox España
T +34 91 515 99 00
E info_spain@hiscox.com
www.hiscox.es

18715 03/18