MailTeck & customer comms

GUÍA PRÁCTICA RGPD/GDPR

CONOCIMIENTO DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Esta es una guía desarrollada en varios capítulos para conseguir un conocimiento práctico del Reglamento General de Protección de Datos (RGPD) o General Data Protection Regulation (GDPR).

El autor es Viktor D' Huys, director de TIC del Grupo Joos, miembro del grupo EFORMA (www.eforma.com), al que también pertenece el grupo MailComms (MailTecK & CustomerComms)

Viktor D' Huys es el director de TIC del Grupo Joos. Es responsable de asuntos que incluyen la seguridad de datos y la coordinación del proyecto GDPR. Es Gerente Certificado de Seguridad de la Información (ISACA) y ha recibido la credencial CIPP/E (Certified Information Privacy Professional/ Europe) de la IAPP (International Association of Privacy Professionals), que es la organización de profesionales de privacidad más grande del mundo.

MailTecK & Customer Comms, conforman el grupo MailComms, empresa tecnológica especializada en soluciones integrales end-to-end para comunicaciones personalizadas multicanal de marketing directo y transaccional, así como comunicaciones y transacciones legales.

Diseñamos, generamos digitalmente y distribuimos las comunicaciones para clientes, pudiendo certificarlas y custodiarlas e incluir firma electrónica, por canales físicos y electrónicos (printing, email, SMS, app, web, contact center y redes sociales). Todo ello integrado con sistemas ERP, SCM, HRM, ECM, CRM/BI y webs. Además, ofrecemos servicios de data quality y analytics.

Hemos desarrollado plataformas propias para la gestión y certificación de comunicaciones (Communicalia y CertySign) en modelo comercial SaaS u Outsourcing.

Estamos avalados por la ISO 27001, siendo además Terceros de Confianza según normativa eIDAS.

Nuestros clientes son empresas de sectores como Seguros, Banca, Energía, Automoción, Telecomunicaciones, Retail, Programas de Fidelización o Grandes Marcas.

ÍNDICE

INTRODUCCIÓN

GDPR: Nuevas normas, nuevos retos

A menos que usted haya estado viviendo bajo una roca durante los últimos meses, seguramente habrá oído hablar del RGPD. La nueva legislación europea sobre protección y tratamiento de datos, conocida formalmente como el Reglamento General de Protección de Datos, entrará en vigor el 25 de mayo de 2018. Por lo tanto, dispone de meses para adaptarse usted y su empresa. Los grupos Joos y MailComms le informarán sobre los aspectos más importantes del RGPD, y le explicarán lo que necesita hacer para preparar su empresa, en nuestro blog.

¿Qué introducirá el RGPD en el camino de las nuevas normas y, lo que es más importante, qué significa esto para su empresa? A través de nuestro nuevo blog, intentamos mantenerle al día y mostrarte que no estás solo, ya que los grupos Joos y MailComms están listos para proporcionar apoyo y compartir su know-how.

Por supuesto, no hay nada nuevo en la legislación sobre protección de datos. El derecho a la privacidad y la recopilación y el uso de datos personales por parte de las empresas han dado lugar a tensiones desde que se adoptó la Declaración Universal de Derechos Humanos en 1948.

La llegada de Internet y los grandes datos ha hecho necesario encontrar un nuevo equilibrio. Aquí es donde entra en juego el RGPD. La UE está introduciendo este nuevo conjunto de normas para garantizar una legislación uniforme en toda Europa. Además, las normas se volverán mucho más estrictas y esto tendrá consecuencias importantes, especialmente para las empresas que recopilan y utilizan datos personales a gran escala o como su negocio principal.

En primer lugar, los datos personales almacenados por su empresa deben estar bien protegidos. Ejemplos de ello son el cifrado de datos en su sitio web, el almacenamiento de datos en ubicaciones debidamente protegidas y la transparencia sobre qué personas de su empresa están autorizadas a acceder a los datos.

También tendrá que ser transparente sobre qué datos almacena, cómo utiliza los datos y los fines para los que se utilizan. Por ejemplo, los visitantes de su sitio web necesitan dar su aprobación para que sus datos puedan ser utilizados para fines anunciados con antelación. Necesitan saber qué datos guarda y qué hacer con los datos. Además, todo el mundo necesita poder ver y cambiar sus propios datos y borrarlos cuando sea necesario. Obviamente, el cumplimiento de estas obligaciones es una tarea importante.

Por último, es necesario contar con un plan de contingencia que se pueda poner en práctica en caso de una vulneración de datos. En algunos casos, la violación de los datos también tendrá que notificarse a la autoridad supervisora e incluso a las personas afectadas. Además, todas las normas se aplican también a todas las empresas que participan, incluidos los subcontratistas.

Los grupos Joos y MailComms están listos para ayudarle a escribir su propia historia de GDPR. Los procesos que deben seguirse para garantizar el cumplimiento del reglamento requieren bastante tiempo y le queda poco.

Los grupos Joos y MailComms están en una buena posición para informarle de todas sus obligaciones en el marco del RGPD, por lo que estamos dispuestos a compartir con usted nuestros conocimientos técnicos y toda la información necesaria. Ambos grupos pueden apoyar a su empresa de varias maneras, por ejemplo, proporcionando un acuerdo detallado de procesamiento de datos. Este acuerdo es jurídicamente sólido y ofrece un buen equilibrio de obligaciones y responsabilidades mutuas.

Proporcionaremos información relevante y una serie de sugerencias y consejos para tratar con el RGPD en otras publicaciones.

CAPÍTULO 1

¿A qué nos referimos cuando hablamos de datos personales?

Es imposible hablar sobre RGPD sin reflexionar sobre la definición de “datos personales”. El RGPD define los datos personales como “cualquier información relativa a personas físicas identificadas o identificables”. Al igual que con todas las definiciones, cada palabra es importante, y por lo tanto, analizaremos a continuación, cada uno de los términos contenidos en la definición anterior.

- Personas físicas: La definición de datos personales abarca los datos sobre las personas físicas que aún viven, pero no los datos relativos a las personas jurídicas. Por lo tanto, excluye a las empresas que son clientes o proveedores, aunque sí incluye los datos de las personas de contacto, por ejemplo.
- Personas identificadas: Una persona puede ser identificada por medio de su nombre, apellido, dirección y fecha de nacimiento, por ejemplo. Cuantos más datos haya recopilado y cuanto más pequeño sea el grupo de personas implicadas, más fácil será rastrear la información hasta un solo individuo.
- Personas identificables: Los datos que no pueden vincularse a una persona pueden contener una clave que permita combinarlos con otros datos. Si esto pudiera dar lugar a la identificación de una persona, los datos en cuestión se consideran datos personales. El RGPD declara explícitamente que tales datos seguirán clasificándose como datos personales, siempre que sea posible combinarlos con cierta facilidad.

- Cualquier información: Este término indica claramente que los datos en cuestión no se limitan a la información digital contenida en las bases de datos. Los datos personales también incluyen información recogida en papel, materiales visuales, grabaciones sonoras y otras fuentes. Algunas de las iniciativas legislativas anteriores se limitaban a la información digital, pero no es precisamente el caso del RGPD.
- Información relativa a una persona: Hay información que, por sí sola, no indica nada sobre una persona, sin embargo puede considerarse como datos personales si está vinculada a ella, por ejemplo, información sobre su ubicación en un momento determinado.

Por lo tanto, el término "datos personales" abarca una amplia gama de datos: nombre, dirección, fecha de nacimiento, estado civil y nombres de su pareja e hijos, el expediente médico que lleva su médico de cabecera y hasta una lista de condenas penales. Sin duda, a menudo facilitamos información voluntariamente sobre cualificaciones, conocimientos de idiomas y experiencia laboral. Es probable que comparta experiencias personales en las redes sociales con amigos y familiares solamente, y no lo haga con el mundo exterior, sin embargo, ¿alguna vez ha considerado datos como la lista de todos los artículos que compró en su supermercado favorito durante el último año o su historial de búsqueda en Internet? Los datos personales incluyen la ubicación exacta de su teléfono móvil en diferentes momentos.

Consejo

Para hacerse una idea de la cantidad de datos que entran en el ámbito del RGPD, trate de enumerar todos los datos personales que se encuentran en tu propio entorno de trabajo, incluyendo los que tiene su empresa y sus contactos de otras compañías. Realice este ejercicio antes de seguir leyendo: ¿Ha terminado su lista? ¿Ha tenido en cuenta los siguientes puntos? Cajones llenos de tarjetas de visita u hojas de cálculo con datos de contacto, los números de teléfono de la casa de sus compañeros o el número personal de un consultor que se lo dio en confianza para casos de emergencia. Fotos tomadas durante la última fiesta del personal. Su CV. Informes de entrevistas de evaluación o valoración. Registros de días trabajados, ausencias y bajas por enfermedad. Imágenes de cámara tomadas en las entradas a los locales comerciales o en el lugar de trabajo. Registros que el departamento de TI mantiene de las horas que usted ha ingresado a la red o aplicaciones específicas, así como los sitios web que visita. Los mensajes de correo electrónico: su contenido, el número de mensajes y los destinatarios. Cuestionarios que usted rellena para recibir información de un proveedor, descargar un libro blanco o suscribirse a un boletín de noticias.

Esta lista muestra claramente por qué se necesita legislación para garantizar que todos aquellos que utilizan datos personales los traten con la debida diligencia y se adhieran a una serie de normas. Al mismo tiempo, también es inevitable e incluso necesario que los datos personales puedan ser utilizados por particulares, el gobierno e incluso empresas. El RGPD pretende garantizar un buen equilibrio entre el derecho a la intimidad de las personas y la posibilidad de que las empresas puedan hacer un uso fraudulento de los datos que disponen.

CAPÍTULO 2
Categorías especiales de datos personales

El RGPD pretende encontrar un equilibrio entre los fines para los que las organizaciones recogen y utilizan los datos personales y el derecho que tienen todas las personas a la protección de su intimidad. La naturaleza y la cantidad de los datos tratados deben ser siempre proporcionales a la finalidad para la que se utilizan.

El grado en que los datos personales son delicados varía ampliamente. Algunos datos personales son conocidos públicamente o son tan difundidos y fáciles de encontrar que su vulneración apenas causaría problemas y no podría considerarse una verdadera invasión de la privacidad. Otros tipos de datos son tan confidenciales que el RGPD ha creado categorías especiales de datos personales, a las que se aplican normas adicionales. Por lo tanto, es crucial que sepa desde el principio si los datos personales que se van a tratar pertenecen a una categoría especial.

El RGPD especifica las siguientes categorías especiales:

- Información sobre el origen racial o étnico.
- Datos relativos a las creencias religiosas o filosóficas.
- Información sobre las opiniones políticas o su afiliación sindical.
- Datos relativos a la vida sexual u orientación.
- Información médica.
- Datos de identificación biométrica y ADN.
- Información sobre condenas penales e infracciones

Como regla general, es mejor no recopilar ni procesar ninguno de los datos anteriores. No obstante, si estos datos han de recogerse y tratarse, deberá registrarse claramente la finalidad y el motivo legítimo para ello, además de cumplirse condiciones específicas para esas categorías especiales. Por lo que se refiere a las distintas fases del procesamiento de datos, también se aplican normas más estrictas en materia de seguridad de la información, transferencia de datos a un lugar fuera de Europa y, en particular, el tratamiento de las infracciones de datos.

Con respecto a los datos personales que no pertenecen a ninguna de las categorías especiales, todavía es posible hacer una distinción entre los datos que tienen un bajo riesgo de invadir la privacidad y la información más sensible. La información financiera, por ejemplo, es más sensible que una dirección y los datos relativos a los niños deben tratarse siempre con especial cuidado.

Por lo tanto, si recopilas y utilizas datos personales, siempre debes considerar si realmente necesitas los datos en cuestión para el propósito previsto, además de las dimensiones

del riesgo de que la privacidad de la persona pueda ser invadida. El riesgo aumenta en consonancia con el número de personas afectadas y la cantidad de datos recogidos sobre ellas.

Así es esencialmente como se realiza la evaluación del impacto sobre la privacidad (PIA). Puede ser necesario establecer un proyecto completo para el PIA o, dependiendo de las circunstancias, una simple valoración de los hechos puede ser suficiente, pero siempre hay que llevar un registro.

Además, se pueden tomar varias medidas para reducir la sensibilidad de los datos personales que se van a tratar.

- La mejor solución es utilizar datos anónimos. Si convertimos los datos en anónimos, haciendo posible que los individuos ya no puedan ser identificados, estos datos no se considerarían personales, y por tanto, no se aplicaría el RGPD.

  Los datos utilizados para la investigación académica deberían ser anónimos en la medida de lo posible, y este enfoque también es adecuado para el procesamiento de datos a gran escala con fines de marketing.

  Uno de los métodos que se puede utilizar es combinar datos para formar grupos. Si se elige este método, la cantidad de datos debe ser lo suficientemente grande como para asegurar que cada grupo contenga siempre un número razonable de individuos, normalmente un mínimo de cincuenta personas. Es necesario tener en cuenta que cuanto más amplia sea la variedad de datos que recopile, más probable será que una persona sea identificable si los datos se combinan.

- Un método comúnmente utilizado es la “pseudonimización”. En este método, todos los elementos de un conjunto de datos que identifican a un individuo son eliminados y reemplazados por una clave sin sentido. El archivo que contiene las llaves se almacena por separado. Aunque estos datos siguen considerándose datos personales, ya que se refieren a una persona identificable, el riesgo de que repercutan en alguna de las personas afectadas es mucho menor. Por lo tanto, la “pseudonimización” es una buena medida de seguridad para los datos sensibles que deben transferirse.

Aunque las definiciones utilizadas en el RGPD para los datos personales, los datos personales sensibles y los que pertenecen a categorías especiales son esencialmente las mismas que las utilizadas en la antigua legislación sobre privacidad, se necesita una buena comprensión de los mismos como punto de partida cuando se valora el impacto del RGPD.

El próximo capítulo ofrecerá un examen más profundo de lo que se entiende por procesamiento en sí mismo y de los roles que la ley reconoce. En este ámbito existen diferencias significativas entre el RGPD y las antiguas normas.

CAPÍTULO 3
Tratamiento de datos y roles relacionados

Para evaluar qué significará el RGPD para su propia empresa o puesto de trabajo, no basta con saber qué datos se clasifican como datos personales, también es necesario tener una buena comprensión de lo que la ley define exactamente con el término "procesamiento de datos". Además es importante conocer los diferentes papeles que desempeñan las partes en el tratamiento de datos personales, éste papel determina en gran medida sus responsabilidades y obligaciones.

Tratamiento de datos

El tratamiento de datos debe considerarse en términos muy amplios. Obviamente, incluye la recogida de datos sobre los datos de contacto, intereses, comportamiento de compra y visitas al sitio web. Estos datos se utilizan en campañas de marketing o ventas. Sin embargo, el procesamiento de datos incluye mucho más que eso.

Cualquier actividad relacionada con datos personales es una forma de tratamiento de datos que se acoge al RGPD. La consulta, la visualización, el almacenamiento, la eliminación y transporte de datos son sólo algunas de las actividades que la ley considera como tratamiento de datos.

Es importante interpretar el tratamiento de datos de manera suficientemente amplia cuando se recopilan listas de actividades de tratamiento de datos que se realizan internamente o se confían a terceros. Una empresa que presta servicios de nóminas de pago a terceros, obviamente procesa datos personales, pero también lo hace el proveedor que recoge papel usado de su empresa, si éste incluye documentos personalizados que contienen datos personales. Sin embargo, el uso privado de los datos personales por parte de las personas no entra en el ámbito del RGPD. Tampoco lo hace el trabajo de los tribunales y las fuerzas del orden, ya que su trabajo se rige por leyes diferentes.

Los roles

La legislación sobre privacidad identifica una serie de funciones con respecto al procesamiento de datos. Las funciones más importantes son las que define el RGPD como controlador de datos y procesador de datos.

El controlador es la persona responsable de recabar datos personales y mantenerlos, con la intención de tratarlos de alguna manera. Debe registrar la finalidad específica del tratamiento de los datos y demostrar que tiene motivos legítimos para ello. Además deberá decidir de antemano qué datos personales son necesarios para el cumplimiento de esta finalidad. Desde el punto de vista jurídico, es crucial que los datos recogidos y procesados se limiten a lo necesario para cumplir el propósito, porque no procesar los datos es la mejor manera de proteger la privacidad.

El controlador también garantiza la seguridad y disponibilidad de los datos, además de que su integridad se mantenga en todo momento, es decir, que no se hayan modificado o borrado erróneamente y que no se haya vulnerado la confidencialidad. Un aspecto crucial

en este contexto es que los datos deben utilizarse exclusivamente para los fines para los que se recogieron.

Por el contrario, la función del encargado del tratamiento de datos implica la adquisición de datos personales y su tratamiento en función de las instrucciones del controlador, que dependerán del objetivo del proceso. El controlador puede asumir este papel, por supuesto, pero si decide utilizar un tercero, éste sólo desempeñará el papel de procesador. Esta distinción fundamental constituye la base de las obligaciones legales. De manera crucial, el RGPD, en contraste con la legislación anterior sobre privacidad, impone obligaciones explícitas al procesador.

Es importante tener en cuenta que no siempre es fácil definir claramente la asignación de tareas. Por ejemplo, es perfectamente posible que un procesador pueda recopilar los datos personales. Esto se debe a que el controlador es capaz de formar al procesador para que recopile, enriquezca y analice los datos personales como parte de su trabajo.

Todos estos son ejemplos de lo que la ley entiende por “tratamiento de datos personales”. El hecho de que una parte recopile datos no lo convierte automáticamente en el controlador. Por el contrario, el cliente de un procesador sigue siendo responsable de los datos incluso cuando las actividades de recopilación de datos se subcontratan al procesador.

En el futuro, será necesario tener un contrato que defina claramente las funciones que desempeñan el cliente y el contratista en el procesamiento de datos. Es una buena idea asegurarse de que este asunto reciba atención constante. La nueva ley supone que el tratamiento de datos se realiza siempre en el contexto de un contrato de tratamiento de datos que establece claramente las obligaciones mutuas con respecto a la privacidad de los datos. Sin embargo, debe ser consciente de si sus responsabilidades están relacionadas con el papel que realmente desempeña, independientemente de si este papel está cubierto por un contrato o no. Esto significa que como procesador necesita asegurarse de no asumir ninguna responsabilidad que no esté de acuerdo con su función. La restricción más importante y obvia es que nunca debe utilizar los datos que el controlador le ha confiado para cualquier propósito que no sea el especificado en las instrucciones del controlador.

Finalmente, la ley define claramente un tercer papel, el del titular de los datos que es la persona a la que se refieren datos personales específicos y quien goza de la protección legal. El RGPD otorga explícitamente a los interesados una serie de derechos en relación con sus datos personales que son fundamentales para el nuevo Reglamento.

En primer lugar, el RGPD exige que los sujetos de datos reciban información clara y transparente sobre el tratamiento de sus datos. Además, también tienen derecho a lo que normalmente se resume como “uso leal” de los datos. Esto incluye la adquisición y el procesamiento legal de los datos, así como la toma de medidas para asegurar que los datos permanezcan exactos, estén adecuadamente protegidos y sólo se utilicen para el propósito indicado. Los interesados tienen derecho a recibir información sobre todos estos aspectos. De esta forma, los propietarios los de datos son, en gran medida, capaces de controlar sus datos individuales pudiendo recuperarlos, corregirlos y borrarlos, así como evitar que sean procesados.

Los derechos y deberes asociados a cada rol serán discutidos en posteriores capítulos.

CAPÍTULO 4

El correcto uso de los datos personales

En este capítulo se examinan los principios básicos del RGPD y las obligaciones resultantes que, como responsable del tratamiento, debe cumplir con respecto al tratamiento de datos personales. También incluye seis pasos que puede tomar para asegurarse de que cumple con los requisitos para mayo de 2018.

El RGPD pretende crear un marco reglamentario que permita a las empresas y organizaciones hacer uso de los datos personales y, al mismo tiempo, garantizar la privacidad de los interesados siempre que sea posible.

Los principios básicos que rigen el uso legítimo de los datos personales son los siguientes:

Debe ser transparente sobre los datos que conserva y las operaciones de tratamiento que lleva a cabo.

- Los datos deben tratarse de manera lícita y justa.
- Debe garantizar los derechos de los interesados.
- Tiene que respetarse la confidencialidad e integridad de los datos
- Debe establecerse la responsabilidad del controlador.

Estos principios de privacidad no son nuevos en la legislación, con el tiempo se han ido definiendo de manera más sistemática y clara. Las obligaciones más importantes que los controladores deben cumplir en el marco del RGPD, se derivan directamente de estos principios.

La transparencia se logra siendo claros sobre los datos personales que guarda, el tipo de tratamiento que lleva a cabo y el objetivo que desea alcanzar al procesar los datos. La información que cubra debe ser fácilmente accesible y estar escrita en un lenguaje claro y directo que pueda ser entendido por todos.

El uso adecuado de los datos personales implica que deben ser recabados de forma lícita, que debe utilizarlos exclusivamente para el fin previsto y que la cantidad de datos recabados, así como el tiempo durante el cual se guardan, no debe exceder de lo necesario para alcanzar dicho fin.

Cualquier persona interesada tiene derecho a recibir información sobre la forma en que procesa sus datos. Pueden pedir que se inspeccionen sus datos individuales y que se corrijan, completen o eliminen. En determinadas circunstancias, un interesado puede impedir el tratamiento de sus datos. Garantizar el respeto de todos estos derechos no es tarea fácil.

Respetar los datos significa que debe hacer todo lo posible para garantizar que los datos se introduzcan correctamente y se mantengan actualizados y seguros, de modo que no

se publiquen o utilicen de forma ilícita para fines indebidos. El responsable del tratamiento debe poder demostrar que cumple todas las obligaciones que le impone el Reglamento y es responsable de las posibles deficiencias.

Evidentemente, todos aquellos que reconocen la importancia de la responsabilidad social de las empresas apoyarán plenamente estos objetivos. Por lo tanto, el RGPD y las explicaciones más detalladas proporcionadas por las autoridades nacionales de supervisión deberían considerarse como una ayuda, en lugar de una forma de imponer restricciones a la privacidad, ya que las empresas y otras organizaciones pueden utilizar estos documentos como una guía para alcanzar objetivos importantes al tiempo que prosiguen sus actividades actuales.

A continuación se resumen brevemente las medidas más importantes que los responsables del tratamiento de datos deben tomar en los próximos meses para garantizar el cumplimiento del nuevo Reglamento antes del 25 de mayo de 2018.

1. Establecer registros de las operaciones de tratamiento de datos personales. Esta es una obligación relacionada con RGPD y, a partir del 25 de mayo de 2018, debe presentar estos registros a la Comisión de Privacidad cuando se le pida. Debería considerar esto como un recurso útil. Esto se debe a que los registros le proporcionarán una imagen de todos los datos personales que utilice. Los registros deberán indicar el tipo de datos de que se trate, el tipo de tratamiento, la finalidad de éste y sus motivos jurídicos.
2. Prepare una declaración de privacidad. Debe ser de fácil acceso siempre que recopile datos de contacto y otra información sobre individuos.
3. Compruebe si tiene la seguridad adecuada para todos los datos personales que recopila. ¿Su red es segura? ¿Cifran los archivos que contienen datos personales o utilizan protección por contraseña? Cuando los datos ya no son necesarios, ¿se eliminan con seguridad? Todo esto se aplica tanto a datos digitales como a datos impresos.
4. Elaborar instrucciones en las que se exponga lo que hay que hacer si el interesado se pone en contacto para ejercer sus derechos, para asegurarse de que pueda tomar las medidas necesarias a tiempo. ¿Quién recibirá la solicitud? ¿Quién hará qué?
5. Elaborar un procedimiento claro que contenga todos los pasos a seguir en caso de que se produzca una vulneración de los datos y exista el riesgo de que se pueda infringir la privacidad de los interesados. ¿Todos sus empleados están al tanto de este procedimiento?
6. Si contrata a terceros para que procesen datos personales, asegúrese de que exista un contrato en vigor que describa claramente lo que el subcontratista tiene que hacer y cuáles son sus obligaciones y responsabilidades en virtud del RGPD.

Cada uno de estos puntos de acción se desarrollará en detalle en futuros capítulos, en el que una discusión general irá acompañada de consejos prácticos. Pero primero examinaremos cómo encontrar la mejor persona de su organización para liderar el proyecto RGPD.

CAPÍTULO 5
¿Necesita un Data Protection Officer?

Existe una gran probabilidad de que el DPO, Data Protection Officer en inglés o traducido a nuestro idioma, Responsable de Protección de Datos ocupe una posición clave en su proyecto RGPD. En este capítulo examinaremos los tipos de empresas que requieren un DPO, así como el papel que desempeña.

El RGPD no requiere que cada controller designe un DPO. Durante mucho tiempo en las conversaciones preparatorias, parecía probable que la obligación de designar un DPO se aplicaría a todas las empresas con al menos 250 empleados, pero este objetivo se abandonó finalmente. La obligación se basa ahora mucho más en la naturaleza del negocio.

Si las actividades de una organización conllevan un riesgo real de infracciones graves de la intimidad, debido a la cantidad de datos tratados, la naturaleza de los datos o la frecuencia de las operaciones de tratamiento, la organización debe disponer de un responsable de la protección de datos (DPO) para asegurarse de que cumple la legislación.

Algunas organizaciones siempre están obligadas a designar un DPO. Este grupo está formado por todas las organizaciones gubernamentales, todas las empresas cuyas actividades principales consisten en el tratamiento de categorías especiales de datos personales, y todas las empresas u organizaciones cuyas actividades principales consisten en la recogida y el tratamiento regular y sistemático de datos personales a gran escala.

Incluso si no tiene ninguna obligación legal de hacerlo, se recomienda que asigne explícitamente el papel de DPO a una persona concreta, ya que esto asegurará que su empresa haya designado a una persona para dirigir los preparativos. El responsable de la protección de datos se asegurará de que exista una cultura de protección de datos dentro de su empresa, de que el asunto de la privacidad de datos se incluya en la agenda y de que su empresa esté preparada para el RGPD a tiempo. El DPO tendrá que disponer de tiempo suficiente para estudiar la legislación y aprender los fundamentos, tras lo cual los conocimientos adquiridos podrán transmitirse al resto de la organización. Y no hace falta decir que el DPO desempeña un papel de liderazgo en el proyecto del RGPD.

Requisitos aplicables al responsable de la protección de datos

Las empresas que tienen que designar un DPO deben tener en cuenta una serie de requisitos:

- El nombre y los datos de contacto del DPO deben comunicarse a la Comisión de Privacidad.
- El responsable de la protección de datos debe tener experiencia en el ámbito de la legislación sobre privacidad, así como un conocimiento profundo de la empresa, sus actividades y el mercado en el que opera.

- También debe tener autoridad suficiente y disponer de recursos suficientes para llevar a cabo su tarea. Se espera que el DPO rinda cuentas a la alta dirección y, por lo tanto, sea suficientemente independiente. Además, no pueden surgir conflictos de intereses. Por esta razón, una persona con responsabilidades en el área de TI no podrá ocupar el cargo de DPO al mismo tiempo, ya que esa persona tendría que comprobar las medidas de seguridad establecidas por su propio equipo.
- Por supuesto, la forma en que se ejerce en la práctica el cargo de DPO depende de la escala de la organización. En las pequeñas empresas, el papel del DPO no será un puesto a tiempo completo, por lo que puede combinarse mejor con otras tareas. También es perfectamente posible que una persona externa desempeñe el papel de DPO.

El RGPD no especifica ninguna cualificación o certificado que deba poseer el DPO, ni tampoco indica si debe darse prioridad a los conocimientos y experiencia jurídicos, organizativos o técnicos. Obviamente, se requiere una cierta cantidad de conocimientos como mínimo incluso en organizaciones pequeñas. Además de los esfuerzos realizados para acumular conocimientos, que se pueden realizar de muy diversas maneras, vale la pena invertir en varios días de formación específica.

El DPO elabora la política de privacidad de datos, que se trata en detalle con la dirección e incluso con el Consejo de Administración. El texto de esta política constituye la base para el resto del proyecto RGPD. Dentro de ese proyecto, el DPO se encarga de la evaluación de las operaciones de tratamiento de datos personales.

Un DPO confiere una ventaja

Por lo tanto, tener un DPO le confiere una ventaja significativa, incluso si no está legalmente obligado a tenerlo en su situación específica. El DPO desempeña un papel en cada uno de los seis pasos preparatorios que se identificaron en el cuarto capítulo.

El DPO también tiene importantes tareas que realizar en otros procedimientos relativos a los datos personales.

- Participa en el establecimiento de todas las nuevas operaciones de tratamiento de datos personales y asesora sobre los riesgos y las medidas de protección de datos que se requieren.
- El DPO también participa en el seguimiento de incidentes e infracciones de datos, y en este contexto es el primer punto de contacto para los clientes, los interesados y las autoridades de supervisión.
- Por último, una de las principales tareas del DPO es garantizar los derechos de los interesados. En este contexto, el DPO actúa como punto de contacto directo para los interesados. Por lo tanto, volveremos a encontrarnos con el DPO muchas veces en futuros capítulos.

Los dos próximos capítulos examinarán más detenidamente la evaluación de los datos personales y los registros de tratamiento de datos personales, ya que constituyen el punto de partida para la preparación del RGPD de todos los controladores.

CAPÍTULO 6

Evaluación de los datos personales y obligación de llevar registros

La mejor manera de empezar a trabajar para garantizar el cumplimiento del RGPD es hacer una evaluación adecuada de los datos personales que su empresa u organización conserva y utiliza. Es posible que también tenga que convertir esta información en registros formales de operaciones de tratamiento de datos personales. Puede ser difícil determinar si tales registros son obligatorios en su situación particular. Por este motivo, en este capítulo intentaremos aportar una aclaración.

Valoración de datos personales

Las grandes organizaciones utilizan programas informáticos especializados para evaluar sus datos personales, aunque una simple hoja de cálculo que contenga la información necesaria puede ser igualmente útil. Usted puede averiguar muchas cosas simplemente haciendo las siguientes preguntas a los departamentos implicados:

- ¿Qué datos personales se recogen y/o utilizan? Categorías de datos, tipos de personas a las que se refieren y número de afectados.
- ¿Cómo se procesan los datos y para qué fin?
- ¿Con qué proveedores, socios u otros terceros se comparten los datos?
- ¿Existen flujos de datos a países fuera de la UE?

A continuación, es necesario determinar si el objetivo para el que se utilizan los datos es legítimo y está en equilibrio con el derecho a la privacidad de los interesados. Por último, es necesario identificar las amenazas existentes para garantizar la confidencialidad e integridad de los datos y las medidas que se tomen para protegerlos. Es un requisito mínimo que todo responsable del tratamiento de datos personales se plantee estas preguntas.

El resultado de este ejercicio le proporcionará la mayor parte de la información que necesita para establecer registros de sus operaciones de tratamiento de datos personales, que es un nuevo requisito impuesto por el RGPD.

Registros de las operaciones de tratamiento de datos personales

La legislación sobre protección de la vida privada existente, o la "antigua", incluye la obligación de comunicar a la autoridad supervisora las operaciones de tratamiento automatizado de datos personales. En España, esta autoridad es la Agencia Española de protección de datos (AEPD). Esta información se introduce en registros públicos que pueden ser vistos por cualquier persona. Sin embargo, este requisito no se aplica a los usos más comunes de los datos personales, tales como la gestión del personal, los registros de nóminas y contabilidad, la gestión de clientes y proveedores, los datos de contacto (siempre que no incluyan información adicional), las listas de miembros de asociaciones y los registros de estudiantes. En consecuencia, la mayoría de las organizaciones no están obligadas a comunicar ninguna información.

Esto cambiará cuando el RGPD entre en vigor y los controladores o responsables de datos tengan que mantener sus propios registros de procesamiento de datos. Estos registros deben estar en formato digital, y debe ser posible presentarlos rápida y fácilmente cuando la AEPD lleve a cabo una auditoría o en el contexto de una investigación de una queja o vulneración de datos (Data breach). Los registros deben demostrar que el responsable del tratamiento tiene una visión clara de los datos personales que procesa. El controlador usa esto para demostrar que ha pensado en su derecho a llevar a cabo las operaciones de procesamiento y que las medidas de seguridad establecidas por el controlador son adecuadas.

Otra diferencia entre el RGPD y la legislación vigente en materia de privacidad es que el RGPD no se limita al tratamiento automático de datos y no prevé una excepción para los "datos personales de uso común".

¿A quién se aplica la obligación?

Se puede hacer una excepción a la obligación de llevar registros para las organizaciones pequeñas hasta cierto punto, aunque el RGPD no está del todo claro en este asunto. Por este motivo, la AEPD publicó recientemente recomendaciones detalladas (el 14 de junio de 2017). A continuación se resumen las recomendaciones más importantes.

Todo responsable del tratamiento, independientemente de que sea una empresa, una organización gubernamental, una asociación o una persona física, debe llevar un registro de sus operaciones de tratamiento de datos personales.

No obstante, se hace una excepción para las organizaciones con menos de 250 empleados y cuyo volumen de negocios sea inferior a 50 millones de euros. Sin embargo, esto no está en consonancia con el espíritu de la ley, ya que todas las medidas deben resultar de la evaluación del riesgo. Cuando una organización pequeña procesa datos personales, esto puede conllevar tanto o más riesgo. Por este motivo, existen muchas situaciones en las que la obligación de llevar registros seguirá vigente, incluso para las PYME.

La obligación de llevar registros no puede evitarse si:

- Los datos tratados se refieren a categorías especiales de datos personales o a grupos de personas particularmente vulnerables, como los niños.
- El tratamiento de los datos entraña riesgos para los derechos y libertades de las personas y, por lo tanto, puede ocasionar un perjuicio físico, material o moral grave. Las recomendaciones contienen una serie de ejemplos: si existe el riesgo de que se pueda vulnerar la confidencialidad de la información financiera o de los datos protegidos por una obligación legal de secreto profesional, si existe el riesgo de robo o fraude de identidad, o si se utilizan datos sobre la salud, la personalidad, el comportamiento o los movimientos, etc., para elaborar perfiles personales.
- El interesado no tiene la posibilidad de ejercer sus derechos personales y, por lo tanto, no tiene ningún control.
- El responsable del tratamiento procesa los datos personales de forma estructural y no ocasional, es decir, el tratamiento de los datos no es un hecho accidental o único, sino "normal". El ejemplo proporcionado en las recomendaciones se refiere a la información relativa a clientes, proveedores y empleados.

Claramente, dibujar una línea divisoria es muy difícil. Cada organización posee algunos datos que podrían causar daños si se vulnerara la confidencialidad, y cada organización conserva algunos datos sobre una base estructural. Por lo tanto, la AEPD recomienda que todas las empresas y organizaciones conserven registros, aunque en el caso de las PYME estos registros pueden limitarse a los datos que se procesan sobre una base estructural. Esto significará que el ejercicio tendrá una escala relativamente limitada en las pequeñas empresas y organizaciones.

En el próximo capítulo se discutirá cómo deberían ser los registros y qué información deben proporcionar sobre cada operación de procesamiento.

CAPÍTULO 7

Registros de operaciones de tratamiento de datos personales

Esta entrega se centra en el contenido de los registros de las operaciones de tratamiento de datos personales. Todos los controladores harían bien en mantener tales registros, aunque, en sentido estricto, no siempre se exige a las pequeñas organizaciones que lo hagan.

En primer lugar, hay que confeccionar una lista sencilla de los datos personales con los que trabaja su empresa u organización, que giran en torno a seis preguntas sencillas: ¿quién?, ¿por qué?, ¿qué?, ¿dónde?, ¿hasta cuándo?, ¿cómo? A continuación se examinan las seis preguntas.

¿Quién?

Primero, sus registros deben establecer quién es el controlador. Esto significa que deben contener información precisa sobre su empresa u organización (incluidos los datos de contacto) y el nombre y los datos de su responsable de protección de datos (DPO). Si no dispone de un responsable de protección de datos, sus registros deben identificar a la persona con la que debe ponerse en contacto en caso de que surjan preguntas, problemas, quejas o infracciones de datos.

Se aconseja a las grandes organizaciones que especifiquen el departamento o la persona responsable de cada conjunto de datos personales. Esto se debe a que el departamento o persona en cuestión actuará como punto de contacto para obtener información sobre otros asuntos que se incluirán en los registros.

¿Por qué?

Es esencial que especifique el propósito para el cual utiliza los datos personales. El principio básico que subyace a toda la legislación en materia de privacidad, y el RGPD en particular, es que la información sólo puede recogerse y procesarse si es estrictamente necesaria para el fin previsto. Obviamente, usted necesita los datos de contacto para comunicarse con sus clientes y proveedores. Además, su empresa tiene que recopilar nombres y direcciones para sus actividades de ventas y marketing. Además, también es deseable enriquecer este tipo de datos básicos con información adicional, como la distribución geográfica de los clientes o los sectores en los que operan.

La AEPD subraya que el propósito debe describirse en los términos más específicos posibles y demostrar claramente la necesidad de procesar la información pertinente. Su documento incluye un apéndice con una lista de propósitos y descripciones más precisas que pueden utilizarse como herramienta.

También es una buena idea considerar los fundamentos legales que su organización tiene para el tratamiento de los datos personales, aunque no es estrictamente necesario incluir esta información en los registros. En algunos casos, estos motivos darán lugar a obligaciones o procedimientos específicos que deberán seguirse. Usted debe agregar inmediatamente esa información a los registros, ya que le facilitará comprobar más tarde si cumple con todas las obligaciones legales.

¿Qué?

A continuación, es necesario registrar las categorías de los interesados, por ejemplo, sus clientes, empleados o visitantes, que constituyen la fuente de los datos personales procesados y que se utilizan para fines distintos. En este punto también es necesario indicar el número aproximado de sujetos de los que disponemos datos, ya que esto puede proporcionarle una idea del impacto en el caso de una vulneración de datos.

Seguidamente, deberá especificar la información sobre los registros que conserva y utiliza. Por ejemplo, ¿guarda y utiliza sólo nombres y direcciones, o también recopila información sobre la edad, sexo, posición e intereses de los interesados?

Es crucial que se explicite si cierta información pertenece a alguna de las categorías especiales, esto se debe a que se aplican reglas y restricciones especiales a dicha información. También es necesario identificar explícitamente cualquier información que no pertenezca a estas categorías especiales pero que pueda considerarse sensible, como la información financiera o los datos relativos a menores.

¿Dónde?

Para cada propósito identificado, los registros también necesitan especificar los destinatarios de la información procesada. Puede enviarse a una persona física, a una institución gubernamental o a un responsable interno o externo. Todos los destinatarios deben ser identificados por su nombre.

Es importante indicar si la información se tratará exclusivamente en el Espacio Económico Europeo. Si los datos terminan fuera del Espacio Económico Europeo, debe garantizar que los datos personales seguirán estando adecuadamente protegidos y que los interesados seguirán disfrutando de los mismos derechos y protección. Esto debe demostrarse en los registros.

¿Hasta cuándo?

Como los datos sólo pueden ser utilizados para el fin previsto, lógicamente no pueden conservarse más tiempo del necesario para ello. La Comisión de Privacidad ha declarado que los períodos de retención no siempre tienen que expresarse como un número específico de días, meses o años, y también son posibles formulaciones tales como “el periodo de retención prescrito por la ley”.

¿Cómo se protegen los datos?

Como controlador o responsable de datos, en el marco del RGPD usted es responsable de la protección de los datos personales que procesa. Debe tomar todas las medidas necesarias para garantizar que su confidencialidad e integridad no se vean comprometidas. Los datos no deben publicarse o transmitirse de forma errónea a los destinatarios equivocados y no deben modificarse de forma indebida.

El mantenimiento de registros completos y exactos le proporcionará una buena base para demostrar que tiene el debido cuidado al tratar los datos personales y que se toma en serio su responsabilidad. También le proporcionará un punto de partida para elaborar sus propios procedimientos internos y comprobar si estos procedimientos se aplican correctamente. Y, por último, también resultará útil cuando redacte declaraciones de privacidad.

CAPÍTULO 8

Base jurídica para el tratamiento de datos personales

Al preparar los registros de las operaciones de tratamiento de datos personales, es aconsejable que los responsables del tratamiento documenten la base jurídica en los registros, aunque no es un requisito. Para que los datos puedan utilizarse legalmente, la operación de tratamiento debe tener una finalidad específica y un fundamento jurídico demostrable. Por otra parte, la operación de tratamiento debe respetar las normas de proporcionalidad y subsidiariedad, lo que significa que debe ser necesaria y proporcionada al fin perseguido.

El RGPD prevé una serie de bases jurídicas potenciales, que no son aplicables en todos los casos. Antes de iniciar una operación de tratamiento, es importante considerar cuidadosamente su base legal. Este procedimiento debe estar documentado y puede desempeñar un papel importante más adelante en caso de que surjan disputas o reclamaciones.

Las instrucciones más claras y específicas proporcionadas por el RGPD en relación con la base jurídica, se refieren al consentimiento del interesado, que discutiremos detalladamente a continuación.

También pueden invocarse otros fundamentos jurídicos. Los datos pueden ser necesarios para la ejecución o preparación de un contrato. Todos los tipos de datos personales son necesarios en el contexto de la relación entre un cliente y un proveedor, en primer lugar y sobre todo son los datos de contacto, pero en el mundo B2C, datos de pago y la información financiera también se requieren con frecuencia. Este fundamento jurídico proporciona una

justificación adecuada en la medida en que se demuestre que la información tratada es necesaria para finalizar el contrato o prestar el servicio acordado.

Una obligación legal también puede servir de base para el tratamiento de datos personales. Esto puede ser una obligación en virtud de la legislación europea o nacional que obliga a las empresas a revelar información al gobierno. Este es el caso de las empresas que incluyen bancos, aseguradoras y compañías aéreas.

El interés público también puede proporcionar una base jurídica, por ejemplo, si el Gobierno acuerda acuerdos organizativos con las empresas a efectos de la administración fiscal. Esta base jurídica también permite la recogida de datos con fines de investigación científica o histórica. Las tareas de las autoridades públicas también están cubiertas por el interés público.

Además, la ley establece que usted puede utilizar los datos personales de un interesado u otra persona física en asuntos relacionados con intereses vitales, es decir, literalmente una cuestión de vida o muerte. En ese caso, debe actuar en interés de una persona individual con suficiente sentido común.

El último fundamento jurídico es el interés legítimo del responsable del tratamiento o de un tercero. Esto no es aplicable a las autoridades públicas. Si se basa en este fundamento jurídico, siempre debe dejar esto claro y sopesar cuidadosamente sus intereses contra el derecho a la privacidad de los interesados. Esto debe ser claramente explicado y demostrado en sus propios registros y en las declaraciones de privacidad que usted redacte a modo de explicaciones para los interesados. Un interés puramente económico ya no constituye una justificación adecuada y la operación de tratamiento debe ser necesaria, cabe señalar que este fundamento jurídico es el más débil.

El RGPD exige específicamente que se preste más atención al tratamiento de datos sobre los niños, hasta los 16 años. Esto requiere el consentimiento de los padres, que no es tan fácil de organizar. Se aplican normas aún más estrictas al tratamiento de categorías especiales de datos personales. El tratamiento de este tipo de datos está prohibido excepto en casos específicos, que se establecen en el RGPD.

Estos casos específicos pueden resumirse como sigue:

- Si los interesados han dado su consentimiento expreso.
- Si los datos de que se trata ya están a disposición del público, puesto que el interesado los ha hecho manifiestamente públicos.
- Si esto se hace en virtud de la legislación laboral. Todos los tipos de datos deben tratarse en relación con la seguridad social, los requisitos legales y los acuerdos contractuales.
- Si se trata de un interés vital y el interesado no puede dar su consentimiento. Esto a menudo se refiere específicamente al uso o la transferencia de datos médicos.
- Si el tratamiento se lleva a cabo para asociaciones sin ánimo de lucro y organizaciones benéficas, en la medida en que el tratamiento se refiera a la utilización legal de datos

sobre los miembros, antiguos miembros o personas con las que la asociación u organización pertinente esté en contacto regular.

- Si el tratamiento se realiza para fundaciones, sindicatos u organizaciones políticas o religiosas (con fines políticos, filosóficos o religiosos).
- En el caso de los datos relativos a delitos o asuntos penales, los datos sólo podrán ser tratados por las autoridades públicas o en los casos previstos por la ley (UE o nacionales). Cada país puede imponer sus propias limitaciones. El derecho penal es un asunto nacional y no está establecido en el RGPD.
- Si los datos son necesarios en el marco de un procedimiento judicial.
- En algunos casos, cuando ello sea necesario por razones de interés público:
  - En caso de un interés público sustancial, y cuando esté cubierto por la legislación comunitaria o nacional que también proteja los derechos de la persona.
  - En el marco de la asistencia sanitaria: diagnóstico médico, datos para la organización de los sistemas y servicios de asistencia sanitaria o social, evaluaciones de la salud de los trabajadores, pruebas de medicamentos…
  - En caso de que los datos sean necesarios para fines de investigación científica o histórica o para fines de archivo, en cuyo caso es necesario tomar las medidas de protección necesarias (los resultados de la investigación pueden ser anónimos o seudonimizados, por ejemplo).

En todos los casos, siempre se requieren motivos importantes para el tratamiento de datos personales. Las razones legales que se desprenden del consentimiento del interesado y el interés legítimo del responsable del tratamiento se tratarán en siguientes capítulos.

CAPÍTULO 9
Consentimiento otorgado por los interesados

La obtención del consentimiento de los interesados constituye la mejor base jurídica para el tratamiento de los datos personales. En la práctica, sin embargo, obtener el consentimiento no es nada sencillo. Además, dado que el consentimiento puede ser revocado en cualquier momento, este fundamento jurídico también entraña un elemento de incertidumbre.

El consentimiento ha desempeñado un papel en la legislación sobre la privacidad durante mucho tiempo, aunque las normas se han vuelto más estrictas a lo largo de los años. Al principio, se permitía extraer algún tipo de consentimiento tácito, a menudo como parte de un contrato más amplio y sin un propósito predeterminado. Posteriormente, se hizo obligatorio permitir que los interesados retiraran el consentimiento (opt out), es decir, la exclusión voluntaria. Hoy en día, el RGPD impone toda una serie de condiciones que deben cumplirse para que el consentimiento sea considerado válido (opting in). El consentimiento debe darse voluntariamente mediante un acto afirmativo, ser informado y ser claro y específico, y debe poder ser retirado con la misma facilidad con que se da.

Voluntario

El consentimiento otorgado por el interesado no puede utilizarse como base jurídica si existe un desequilibrio en la relación entre el responsable del tratamiento y el interesado. Esto se aplica en el caso de la relación entre un empleado y un empleador, por ejemplo, porque el empleado no suele estar en condiciones de negarse a dar su consentimiento.

Además, el consentimiento no podrá vincularse a la prestación de un servicio a menos que los datos sean necesarios directamente para el cumplimiento del contrato. En ese caso, sin embargo, la necesidad contractual constituye el fundamento jurídico, por lo que, en aras de la claridad, es mejor no solicitar el consentimiento. Además, el consentimiento para la utilización de los datos en posteriores campañas de marketing y publicidad no podrá formar parte de ningún contrato que deba celebrarse ni de ninguna condición general. Dicho consentimiento sólo es válido en el marco del RGPD si puede proporcionarse por separado de la celebración del contrato.

Afirmativo

Los interesados deberán hacer ellos mismos una declaración clara o realizar un acto afirmativo que indique su consentimiento para una operación de tratamiento determinada. Para ello podrá utilizarse cualquier enfoque o método adecuado. El RGPD resume los métodos más comunes, que consisten en dar su consentimiento mediante una declaración oral o escrita, marcar una casilla y activar un parámetro en un navegador o aplicación. Una novedad en esta área del consentimiento es que el RGPD especifica explícitamente que el silencio y la inactividad no pueden constituir consentimiento. Por ejemplo, las cajas precalificadas están absolutamente prohibidas. El no hacer uso de una función opt-out o de un botón unsubscribe tampoco constituye un consentimiento válido. Esta es una condición

extremadamente importante para todas las organizaciones que organizan campañas de marketing directo.

Informado

Antes de solicitar el consentimiento de los interesados, se les debe facilitar información detallada sobre la identidad del responsable del tratamiento, las operaciones de tratamiento previstas, el objeto y la base jurídica y las medidas adoptadas para proteger sus datos. Esto debe hacerse de manera honesta, utilizando un lenguaje claro y sencillo. La finalidad, los datos precisos que se requieren para tal fin y el consentimiento que debe darse deben estar claramente alineados. Una declaración de privacidad detallada y exhaustiva es un documento adecuado para dicha comunicación. La información que debe incluirse en la declaración de privacidad y la mejor manera de ponerla a disposición de los interesados se tratará en otro artículo más adelante.

Específico e inequívoco

El consentimiento para el tratamiento de datos personales se otorga siempre con una finalidad clara. Por lo tanto, el responsable del tratamiento no puede utilizar los datos para ningún otro fin, a menos que el nuevo objetivo se asemeje mucho al original. Un buen ejemplo de tal propósito es contactar a clientes antiguos o existentes para informarles acerca de un producto o servicio que está estrechamente relacionado con un producto o servicio que ya han comprado.

Debe prestar especial atención si está considerando combinar los datos de una manera diferente o utilizarlos para un propósito completamente distinto. La minería de datos es un problema en este contexto. Esta tecnología se utiliza a menudo, entre otras cosas con fines de marketing, para descubrir patrones potenciales o asociaciones inesperadas en grandes cantidades de información, por lo que no existe un propósito predeterminado. El RGPD ofrece cierto margen de flexibilidad en los casos en que los datos se reutilizan y el consentimiento explícito de los interesados puede solicitarse la próxima vez que se utilicen los datos.

El consentimiento puede ser revocado

En todo caso, debe informarse a los interesados de que pueden revocar su consentimiento en cualquier momento. El procedimiento para retirar el consentimiento debe ser tan simple como el procedimiento para otorgar el consentimiento. Bajo el RGPD, el controlador está ahora específicamente requerido para facilitar esto.

Si bien este enfoque es justo y lógico, poner en práctica esta obligación no siempre es sencillo, sobre todo porque el RGPD exige que el responsable del tratamiento pueda demostrar claramente que los interesados dieron su consentimiento. En futuras capítulos se ofrecerán consejos más específicos al respecto.

CAPÍTULO 10
Consentimiento o interés legítimo

En anteriores capítulos de esta guía, hemos analizado las diferentes bases jurídicas posibles que existen para el tratamiento de datos personales. En algunos casos existen varios fundamentos jurídicos en los que se puede confiar. Pero, ¿cómo elegir la mejor base jurídica para justificar sus operaciones de tratamiento?

Responder a esta pregunta es más difícil de lo que parece. Sin embargo, es importante tomar tiempo para considerar este aspecto porque la elección que usted hace tiene consecuencias. Algunos fundamentos jurídicos ofrecen más seguridad a largo plazo que otros. Sin embargo, cambiar entre diferentes bases jurídicas posibles causa confusión y puede crear la impresión de que se está intentando engañar a los interesados.

La elección de la base jurídica es clara siempre que los datos en cuestión se traten con el fin de prestar los servicios acordados en virtud de un contrato, por ejemplo, datos de contacto para pedidos, entregas o prestación de servicios y facturación, o en relación con obligaciones legales. Sin embargo, es mucho más difícil elegir entre obtener el consentimiento de los interesados y basarse en un interés legítimo.

Solicitar el consentimiento de los interesados siempre parece ser una buena opción, pero también entraña riesgos. Si usted solicita el consentimiento pero no lo obtiene, esto significa que ya no está autorizado a procesar los datos pertinentes. Imagine que está planificando una campaña de marketing y envía una carta o correo electrónico a todas las personas incluidas en un archivo para solicitar el consentimiento explícito de contactarlos en el futuro. Como la tasa de respuesta a este tipo de comunicación es tal vez alrededor del 10%, el resultado sería que ya no podría utilizar la gran mayoría de sus contactos.

Naturalmente, usted estaría seguro en aquellos casos en los que pudiera demostrar que ha obtenido dicho consentimiento. Obtener el consentimiento también le permitiría crear una imagen positiva, comunicando abiertamente sus intenciones y teniendo en cuenta las preferencias de sus contactos. Al mismo tiempo, sin embargo, dificultaría la amplia difusión de sus campañas y haría extremadamente difícil añadir nuevos destinatarios. Por último, siempre existiría el riesgo de que en algún momento los interesados se retractaran de su decisión y retiraran su consentimiento, lo que provocaría una mayor erosión de su base de datos.

En ese caso, ¿cuáles son las alternativas? Siempre puede confiar en el interés legítimo de su organización como fundamento jurídico. Para continuar con el ejemplo de una campaña de marketing, una organización comercial no puede funcionar si no tiene la oportunidad de presentar y anunciar sus productos. Como se mencionó anteriormente, usted tiene que armar su caso cuidadosamente. En primer lugar, los datos que se utilizarán para el tratamiento deben limitarse a los estrictamente necesarios. Tener menos información reduce automáticamente el riesgo de una violación grave de la privacidad. Un archivo que sólo contiene detalles de contacto obviamente no es tan crítico como un gran conjunto de datos que incluye datos confidenciales.

A continuación, debe tomar todas las medidas necesarias para proteger adecuadamente los datos y garantizar la confidencialidad. Usted tiene que demostrar que los datos recogidos no pueden ser utilizados para otro propósito. Esto le permitirá mantener un equilibrio entre los intereses de los interesados y los de su propia organización. Es mejor guardar notas breves (o notas más detalladas, si es apropiado) de la línea de razonamiento que siguió en sus registros. En ese caso, en caso de que surjan disputas más adelante, siempre podrá demostrar que ha actuado de buena fe y ha considerado los asuntos correctos.

Lamentablemente, incluso si se adoptan todas estas medidas, no se puede descartar la posibilidad de que un interés legítimo que se utilice como fundamento jurídico pueda ser impugnado en cualquier momento. Un interesado que sienta que ha sido tratado injustamente o un competidor que piense que usted sigue prácticas desleales puede presentar una queja a la AEPD, que puede conducir a una investigación y posiblemente a una acción legal. El resultado de cualquier acción legal dependerá de cómo los auditores o el tribunal interpreten los hechos específicos, y esto puede, por supuesto, ser diferente de su propia evaluación. En ese caso, es posible que se le imponga una multa o se le prohíba el procesamiento de datos, y es posible que tenga que pagar daños y perjuicios. A la hora de pronunciarse y decidir sobre las medidas correctoras que deben adoptarse, la AEPD tendrá en cuenta la situación general. Los hechos tendrán más peso en el caso de una organización que no haya implementado adecuadamente ningún aspecto de la legislación sobre privacidad. Sin embargo, si usted ha tomado las medidas necesarias y puede presentar argumentos claros sobre por qué cree que determinadas operaciones de tratamiento están justificadas, los hechos no serán contundentes en su contra.

Somos conscientes de que esta no es una respuesta clara y no hemos proporcionado una directriz directa, pero la privacidad es un derecho que debe sopesarse con otros derechos y siempre será objeto de interpretación y debate. Dicho esto, el sentido común y un enfoque honesto y abierto contribuyen en gran medida. Lo siguiente que necesita hacer es comunicar claramente y documentar adecuadamente la perspectiva que ha adoptado. Y no hace falta decir que necesita tomar las medidas de seguridad esperadas a lo largo del proceso de procesamiento de datos para limitar el riesgo de violaciones de datos.

CAPÍTULO 11

¿Qué es una declaración de privacidad y qué debe contener?

En los anteriores capítulos hemos analizado detalladamente los registros de las operaciones de tratamiento de datos. Es necesario llevar un registro de los datos personales que procesa su organización, el propósito para el cual se procesan estos datos y la base legal para estas operaciones de procesamiento. A partir del 25 de mayo de 2018, toda organización estará obligada a conservar dichos registros. Estos registros pueden resultar muy útiles de muchas otras maneras. Constituyen el punto de partida perfecto para llevar a cabo una evaluación de riesgos y producir una visión general de las medidas de protección de datos y procedimientos internos de su organización. Lo estudiaremos con más detalle en siguientes capítulos. Además, los registros bien conservados le proporcionan la información que necesita para informar a los interesados sobre el tratamiento de sus datos, que es el tema de este capítulo.

El RGPD requiere que se proporcione información transparente a todos los interesados, es decir, a todas las personas cuyos datos utilice. Los interesados tienen derecho a conocer las operaciones de tratamiento en las que se utilizan sus datos. El texto en el que una organización publica esta información se conoce como “declaración de privacidad”.

Cada uno de estos elementos debe estar cubierto en la declaración de privacidad:

- El responsable del tratamiento debe identificarse mediante el nombre oficial de la empresa u organización en cuestión, la dirección completa de su domicilio social. Si la organización ha designado un responsable de protección de datos (DPO), la declaración de privacidad también debe proporcionar información sobre cómo ponerse en contacto con esta persona. Deberá facilitarse como mínimo una dirección, un número de teléfono o una dirección de correo electrónico a través de los cuales pueda ponerse en contacto con el responsable de la protección de datos, pero no es necesario facilitar su nombre. Las organizaciones que no tengan un DPO deben dirigirse a un punto de contacto.
- La parte más importante de la declaración es la lista de las operaciones de tratamiento de datos personales llevadas a cabo por su organización. Las operaciones de tratamiento deben describirse con suficiente detalle, con listas separadas para cada fin. Cada vez, usted debe indicar el propósito para el cual se recogen los datos específicos, las categorías de datos que usted procesa y las categorías de personas implicadas, las operaciones de procesamiento que se llevan a cabo y la base legal en la que usted confía para poder procesar los datos. Al elaborar esta lista, por supuesto, puede recurrir a sus registros internos para asegurarse de que no omita nada.
- También debe ser claro sobre los destinatarios de la información, es decir, quién tendrá acceso a ella y a quién se la transmitirá. Debe indicar qué categorías de empleados están implicados en el tratamiento de los datos y, por lo tanto, pueden acceder a la información y si hay partes externas implicadas en las operaciones de tratamiento de datos. En caso de que la información recogida se transmita a terceros para su

uso posterior, deberá indicarse expresamente. Esto se hace normalmente utilizando términos generales como “empresas del grupo” o “socios”. El RGPD espera que sea lo más transparente posible, ya que es importante que los interesados comprendan dónde acaban sus datos, aunque obviamente no se puede esperar que enumere los nombres completos de cada uno de sus socios o proveedores.

- Debe demostrar que se han tomado las medidas de seguridad adecuadas para garantizar la confidencialidad e integridad de los datos. Una vez más, usted no tiene que entrar en detalles sobre todas las tecnologías y procedimientos implicados, ya que esto obviamente socavaría las medidas de seguridad, pero debería revelar los principios que ha seguido y cómo puede protegerlos dentro de su empresa u organización.
- Una obligación específica es la de a proporcionar información sobre el tiempo de retención (duración de los datos). El RGPD establece que usted puede utilizar los datos personales sólo para el propósito previsto, y por lo tanto no puede conservar los datos más tiempo del necesario para ese propósito. Además, como responsable del tratamiento de datos debe garantizar la calidad de los datos. Esto incluye garantizar que los datos no sean obsoletos. La información sobre el tiempo de retención debe proporcionarse por separado para cada propósito.
- Además, la declaración de privacidad también debe establecer claramente los derechos de los interesados. Estos pueden presentar una queja a la AEPD en cualquier momento si consideran que los datos se están procesando de manera incorrecta. Podrán solicitar al responsable del tratamiento que facilite información sobre las operaciones de tratamiento que utilicen sus datos, debiendo explicarle cómo hacerlo. Y pueden inspeccionar la información disponible sobre ellos personalmente y realizar los arreglos necesarios para que sea modificada o borrada si así lo desean.
- Por último, el RGPD exige que especifique si transfiere determinados datos fuera de la UE. En ese caso, existen riesgos adicionales en relación con la protección de datos y los derechos de los interesados. Estos riesgos incluyen los poderes que tienen las autoridades extranjeras, como la NSA en los Estados Unidos. Se aplican otras garantías, dependiendo del país al que se exportan los datos o del sector en el que opera la empresa u organización. Se trata de un tema muy complejo desde el punto de vista jurídico. En la mayoría de los casos, todo lo que tendrá que declarar es que los datos permanecerán en la UE y, por lo tanto, seguirán disfrutando de la plena protección jurídica que ofrece el RGPD. En caso contrario, deberá especificar dónde se enviarán los datos y la forma de protección que se aplicará. Los interesados pueden entonces decidir por sí mismos si sus datos serán suficientemente confidenciales.

Además de especificar lo que debe contener la declaración de privacidad, el RGPD también proporciona directrices para su diseño y estructura. Los aspectos importantes incluyen la forma en que se comunica la información a los interesados, cuándo la presenta y cómo la mantiene actualizada. Estos aspectos serán considerados en el próximo capítulo.

CAPÍTULO 12

¿Cuál es la mejor manera de presentar una declaración de privacidad?

En el capítulo anterior de esta guía hemos repasado las diferentes cuestiones que deben incluirse en una declaración de privacidad para garantizar que todos los interesados han sido correctamente informados sobre las operaciones de tratamiento realizadas con sus datos. La forma en que se realice también es importante, y los redactores del RGPD han prestado especial atención a este asunto.

Como responsable del tratamiento de datos, su deber es proporcionar esta información de forma concisa y en un lenguaje claro. Algunas empresas se han destacado en la producción de textos complicados, a menudo de decenas de páginas, con formulaciones incomprensibles para el Lego, que disuaden a los usuarios de leer el documento y son la antítesis de la transparencia. El RGPD espera que usted utilice un lenguaje sencillo que pueda ser entendido por casi todo el mundo. En algunos países de la UE, se recomienda específicamente niveles equivalentes al nivel de la escuela primaria. Si su audiencia incluye a cualquier niño, es particularmente importante que usted explique de manera sencilla y clara las aplicaciones de los datos que le proporcionan. Elaborar una declaración de privacidad separada para los niños es a menudo la mejor solución.

La transparencia también puede mejorarse proporcionando un esbozo de los principales elementos en primer lugar y garantizando que el texto tenga una buena estructura. Por ejemplo, puede describir cada tema en una oración o un párrafo breve, y luego dar a los visitantes la opción de hacer clic para obtener más información. De esta manera, los usuarios pueden encontrar rápidamente los artículos que están buscando y aprender más

si así lo desean. Puede ser una buena idea usar iconos para que el mensaje se pueda comunicar de forma más sencilla que con palabras solamente. Hay grupos de trabajo que han estado trabajando en el desarrollo de iconos específicos durante años, pero esta tarea está resultando un reto.

No olvide incluir la fecha y el número de versión en su declaración de privacidad. Los textos de este tipo no son fijos, ya que la naturaleza de los datos que usted procesa, los destinatarios o las medidas de protección adoptadas pueden variar. Su texto debe proporcionar información precisa y actualizada, por lo que se modificará con frecuencia. También se supone que debe mantener informados a los interesados sobre estos cambios. Como mínimo, debe dejarles claro que la declaración de privacidad puede cambiar en el futuro. Pídales que visiten la página de su sitio web regularmente. Vale la pena conservar las versiones antiguas de su declaración de privacidad para que, si se cuestiona una operación de tratamiento, pueda comprobar qué información estaba disponible para los interesados en el momento en que se llevó a cabo la operación de tratamiento relevante.

La forma que su declaración de privacidad debe tomar y el mejor lugar donde publicarlo, dependen de las circunstancias. Necesita asegurarse de que sea fácilmente localizable. Debe evitar ocultar su declaración de privacidad entre sus términos y condiciones generales. Mientras que el método más común es proporcionar un enlace en el sitio web, una declaración de privacidad también puede ser comunicada en papel o incluso oralmente. Sin embargo, hay una serie de reglas que debe tener en cuenta.

Si usted permite que los usuarios introduzcan datos personales en un sitio web o en una aplicación, debe asegurarse de que la información requerida sobre el procesamiento de datos se proporciona primero. La mejor manera de hacerlo es hacer referencia a la declaración de privacidad en la introducción a la aplicación en cuestión. Muchos sitios web hacen esto en un banner al final de cada página. Esto, por supuesto, no es muy específico y no se relaciona con un solo propósito, pero si asegura que la información sea accesible para los visitantes tan pronto como ingresen a su sitio web. Esto es importante para los sitios web que utilizan cookies u otras herramientas para recopilar información sobre el comportamiento de navegación de los visitantes. En el momento que comiencen a trabajar, tan pronto como se ingrese al sitio web, los visitantes deben ser notificados inmediatamente.

Ciertamente no hay nada malo en hacer varias declaraciones de privacidad que se adapten a diferentes grupos objetivo. Es probable que sus clientes actuales o potenciales no estén interesados en la forma en que su organización trata los datos del personal, por lo que utilizar declaraciones de privacidad diferentes le permite ajustar la longitud del texto.

De hecho, el RGPD ofrece una excelente oportunidad para que todas las organizaciones examinen su política de tratamiento de los datos de personal y reflexionen al respecto. El volumen de datos sobre el personal en circulación es mayor de lo que usted imagina e incluye datos sensibles.

El procesamiento de la nómina requiere todo tipo de datos: salario, asistencia, baja por enfermedad y composición de la familia. En muchas empresas, esta información es procesada externamente. Además, los datos deben transmitirse al Gobierno para fines de seguridad social y administración fiscal.

Los archivos de personal de la organización contienen todo tipo de datos relacionados con la carrera profesional. Las personas ajenas al departamento de recursos humanos también tienen acceso a esta información en relación con las actividades de contratación, las evaluaciones y los ascensos. Es importante que realice las mejoras necesarias en los procedimientos de confidencialidad.

Otros datos disponibles se refieren al uso de herramientas informáticas. Éstos pueden ir desde el contenido de los correos electrónicos hasta cuentas de usuario, grupos de usuarios, niveles de autorización y registros del uso de aplicaciones o visitas a sitios web. Es importante que proporcione información transparente sobre los datos registrados y el propósito relacionado. Usted también necesita dejar claro lo que el empleador puede y no puede hacer con esta información.

Las organizaciones más grandes tienen que discutir este tema con el comité de empresa. Los empleados de las empresas más pequeñas también deben ser informados sobre todas las operaciones de tratamiento que utilicen datos personales. Esto se puede hacer en forma de declaración de privacidad interna, que puede incluir en sus términos y condiciones de empleo, o bien distribuir como documento separado, ya sea en papel o en formato digital. No es mala idea pedir a sus empleados que firmen este texto para indicar que lo han leído.

Si bien a veces puede ser necesaria una mayor creatividad, cada organización puede, con algunos esfuerzos, arrojar luz sobre las operaciones de tratamiento de datos personales que lleva a cabo y las razones por las que son necesarias, ya que la transparencia es un requisito básico. Nuestros próximos capítulos considerarán lo que el RGPD quiere decir con medidas adecuadas para proteger los datos personales que se procesan. Esto podría representar un reto importante para muchas empresas.

CAPÍTULO 13

Seguridad adecuada de los datos personales

Hasta ahora, hemos examinado principalmente las directrices de RGPD para el tratamiento real de datos personales, incluidas las condiciones para procesar datos y cómo comunicarse adecuadamente con los interesados. Además de esto, el RGPD requiere que usted proteja adecuadamente los datos contra riesgos durante el procesamiento y en cualquier otro momento.

Si bien la legislación anterior ya incluía una obligación en materia de seguridad de la información, la responsabilidad de la seguridad de la información, que antes estaba restringida al responsable del tratamiento, recaerá también en todos los encargados del tratamiento que traten datos personales siguiendo las instrucciones de un responsable del tratamiento.

Para poder explicarle cómo puede cumplir con esta obligación, primero tenemos que considerar qué implica la seguridad de la información. Obviamente, las organizaciones más grandes y también las empresas que manejan datos confidenciales en nombre de sus clientes de forma sistemática (como los Grupos Joos y MailComms), tienen mucha experiencia en esta área. Existen muchos estándares diferentes para la seguridad de la información, de los cuales el más conocido es la certificación ISO 27001, y existe una amplia gama de documentos políticos, procedimientos e instrucciones operativas para ayudar a las organizaciones y a su gestión, que pueden considerarse una “ciencia” en sí misma. Aquí, sin embargo, consideraremos los principios básicos.

En primer lugar, es necesario identificar las amenazas a las que están expuestos los datos personales (como todos los demás datos confidenciales) y de las que requieren protección.

Muchas personas se refieren en este contexto a los principios de la CIA (cualquier semejanza con una organización estadounidense conocida es pura coincidencia). En este caso, la CIA es sinónimo de confidencialidad, integridad y disponibilidad (Confidentiality, Integrity and Availability). La seguridad de la información garantiza la confidencialidad, integridad y disponibilidad de los datos.

Garantizar la confidencialidad significa garantizar que los datos no se hagan públicos y no queden en manos de nadie más que el destinatario previsto. Todos conocemos ejemplos notables del robo de cientos de miles de datos de tarjetas de crédito o de la publicación de documentos confidenciales por parte de piratas informáticos. Sin embargo, las infracciones de datos pueden adoptar formas mucho más pequeñas, como una carta que termina en el buzón equivocado o un correo electrónico que se envía al destinatario equivocado, ya sea deliberadamente o accidentalmente.

Proteger la integridad de los datos significa que no se puede modificar o borrar ningún dato de forma incorrecta. La falsificación puede ser un caso sencillo de fraude. Los hackers son capaces de manipular datos, pero los cambios involuntarios son mucho más frecuentes como resultado de errores humanos cometidos al escribir software o al configurar sistemas o aplicaciones.

Por último, es necesario garantizar la disponibilidad de los datos. Medidas como las copias de seguridad o un plan de recuperación ante desastres están diseñadas para garantizar que los datos no se pierdan y puedan visualizarse y procesarse cuando sea necesario.

Un programa de seguridad de la información ayuda a tomar los pasos necesarios de manera sistemática. Debe ser consciente de los riesgos específicos a los que están expuestos los datos e intentar eliminar o limitar estos riesgos o reducir su impacto.

El RGPD no especifica exactamente qué medidas son necesarias para garantizar una seguridad adecuada. Esto se debe a que el enfoque apropiado depende de muchos aspectos, los riesgos no siempre son los mismos:

- El impacto de cualquier vulneración de los datos se determina tanto por la cantidad de datos como por su naturaleza: categorías especiales, datos sensibles o datos de identificación frente a datos cuasi públicos.
- La propia naturaleza de la operación de tratamiento puede conllevar riesgos específicos. Por ejemplo, se debe prestar más atención a los análisis de datos automáticos que se utilizan como base para la toma de decisiones.
- El intercambio o transferencia de datos puede crear riesgos adicionales.
- La participación de terceros en la operación de tratamiento puede suponer una amenaza adicional.
- La misma protección no se aplica fuera de Europa.
- El tiempo durante el cual se conservan los datos también puede jugar un papel importante.

- Por otra parte, la ciencia y la tecnología no se quedan inmóviles. Esto significa que lo que hoy en día se considera seguridad adecuada puede dejar de considerarse adecuado dentro de dos años.

Por lo tanto, se trata de encontrar un equilibrio entre los costes y el esfuerzo que implica la adopción de medidas específicas y deben ser proporcionales a la naturaleza de los datos y al daño que podría ocasionar si algo sale mal.

Las organizaciones más grandes, sin duda, ya aplican muchos procedimientos. Formulan su política de seguridad de la información y disponen de un sistema de gestión, identifican los riesgos y consideran si son aceptables, elaboran procedimientos e instrucciones, llevan a cabo comprobaciones y gestionan la realización de auditorías externas, analizan incidentes y aprenden del funcionamiento actual de los procedimientos para poder avanzar en las mejoras. Todos estos pasos se incorporan a las normas de la certificación ISO 27001, por ejemplo.

Si ya dispone de un sistema de gestión de este tipo en funcionamiento, no necesitará tomar muchas medidas adicionales para garantizar que la seguridad de su información está preparada para el RGPD. Obviamente, debe asegurarse de que todos los datos personales se clasifican como confidenciales y que los procedimientos para el tratamiento de datos confidenciales son aplicables a los mismos. Es probable que también se requieran algunos procedimientos adicionales para mejorar las disposiciones relativas a operaciones específicas de tratamiento de datos personales. Sin embargo, aparte de esto, el marco general será aplicable.

Las empresas u organizaciones que no están bien centradas en seguridad de la información se enfrentan a un reto mucho mayor. Por lo tanto, en los próximos capítulos se darán consejos sobre cómo tratar la seguridad de la información en las pequeñas organizaciones, incluyendo cómo minimizar el riesgo de incidentes que impliquen datos personales, desarrollando procedimientos prácticos y aplicando medidas de forma pragmática con sentido común, y cómo demostrar que lo ha hecho de forma adecuada.

CAPÍTULO 14

Evaluación del riesgo de los datos personales

El RGPD hace gran hincapié en el hecho de que todos los responsables del control y tratamiento de datos personales deben proteger adecuadamente la confidencialidad, integridad y disponibilidad de los datos personales. Incluso si no dispone de personal especializado que se ocupe de esta obligación, es perfectamente posible cumplirla con un enfoque simplificado.

El punto de partida para todas las medidas es una evaluación del riesgo. Aunque esto suena difícil y serio, no tiene por qué ser complicado. Simplemente tome registros de las operaciones de procesamiento de datos y revíselos, paso a paso, y hágase algunas preguntas específicas. Luego, agregue dos columnas más a sus registros. En estas columnas, especifique los riesgos asociados con cada operación de tratamiento específica y las medidas que puede tomar para limitarlos.

Daré algunos ejemplos sencillos que es probable que usted también encuentre en sus propios registros. Dispondrá de un conjunto de datos con la información de contacto de las personas a las que les gustaría enviar información sobre sus productos y servicios de vez en cuando. Obviamente usted tiene datos sobre su nombre y dirección, y también sobre el negocio para el que trabaja, sus cargos y quizás sus estudios, pasatiempos y áreas de interés. Además, dispondrá de todo tipo de datos relativos a sus propios empleados.

Usted mantiene información actualizada sobre su desarrollo profesional y evaluaciones anuales. Cada mes, usted proporciona a la Seguridad Social los detalles de los empleados que estaban de baja o enfermos. Hay que conocer la composición de sus familias, porque esto hay que tenerlo en cuenta a la hora de calcular el impuesto sobre nóminas. Y quizás,

sus cámaras de seguridad filman a todos los que entran y salen de sus instalaciones. Existen muchos otros ejemplos, y es imposible concebir situaciones en las que no se procesen datos personales.

¿Cuáles son los riesgos que existen con respecto a la seguridad de esta información? En gran medida depende de cómo se almacenen los datos, es decir, de la tecnología que se utilice.

Si trabaja con archivos de papel, es importante tener en cuenta si las carpetas y los archivos son accesibles en su escritorio o si están guardados en un armario. En este último caso, es necesario identificar quién tiene acceso a su oficina y quién puede coger las llaves. ¿Cierra la puerta cuando se va? ¿Guarda los papeles?

En el caso de los archivos almacenados en un ordenador, se aplican esencialmente las mismas preguntas, aunque las respuestas serán un poco más complejas. Quizá trabaje sin conexión en un ordenador portátil. ¿Tiene este ordenador una contraseña? ¿Eres la única persona que conoce esta contraseña? ¿Son los datos personales confidenciales contenidos en un fichero protegido por contraseña? Cuando saque su ordenador portátil de las instalaciones del negocio, ¿tiene alguna protección adicional? ¿Lo deja a veces en su coche? ¿Dónde lo guarda en su casa?

La situación es otra vez diferente si los datos se almacenan en un servidor en lugar de localmente. ¿Todos los usuarios del servidor tienen acceso a todos los datos? ¿Realmente requieren esto? ¿Puede dividir el servidor en zonas y asignar diferentes niveles de autorización a diferentes usuarios o grupos? ¿Se realiza una copia de seguridad del servidor y dónde se guardan las copias de seguridad? ¿Existe una empresa informática que realiza trabajos de mantenimiento en el parque de servidores? ¿Tiene acceso a todos los datos? ¿Ha llegado usted a un acuerdo con la empresa sobre lo que sus empleados pueden y no pueden hacer, a pesar de que efectivamente tienen todos los derechos que requieren para realizar su trabajo?

¿Están los datos almacenados en la nube? En ese caso, ¿dónde se encuentran los datos y quién tiene acceso a ellos? ¿Qué garantías ofrece el proveedor de Cloud Computing? ¿Se transfieren datos al extranjero o incluso fuera de Europa, donde no están protegidos por el RGPD? ¿Se transfieren los datos de forma segura?

¿Se guardan y almacenan las imágenes de la cámara de seguridad? ¿Cuánto tiempo se guarda? ¿Quién puede ver los datos y en qué circunstancias se consultan realmente?

Como puede haber deducido de las preguntas anteriores, al tomar medidas en cada una de estas situaciones puede reducir drásticamente el riesgo de violaciones e infracciones. Los ejemplos también muestran que los riesgos difieren según el contenido exacto de los archivos. Si un archivo contiene sólo los datos de contacto, una violación de la confidencialidad no tendrá un impacto enorme. Sin embargo, este no es el caso cuando se trata de determinados tipos de datos personales. Se requiere una seguridad mucho más estricta si, por ejemplo, usted trabaja en el sector sanitario y lleva registros de datos

confidenciales relativos a pacientes o clientes (que equivalen a datos médicos) precisamente porque una violación de la confidencialidad o integridad puede tener consecuencias mucho más graves.

Dependiendo del tamaño de la base de datos, el impacto puede ser mayor a medida que aumenta el número de sujetos de datos. Las medidas que usted adopte en relación con cada uno de los riesgos enumerados deben ser siempre proporcionales a la evaluación del riesgo.

Teniendo esto en cuenta, es lógico que el RGPD imponga mayores obligaciones a todas las organizaciones que utilizan categorías especiales de datos personales y a todas las organizaciones que procesan sistemáticamente datos personales como su actividad principal. En algunos casos, es preciso elaborar una evaluación formal del impacto de la protección de datos (DPIA - data protection impact assessment) y presentarla a la AEPD (Agencia Española de Protección de Datos) antes de que se lleve a cabo el tratamiento.

Es aconsejable que todas las empresas y organizaciones realicen en gran medida el mismo ejercicio. También se recomienda que conserve las notas y registros adecuados de los hallazgos, para que pueda demostrar en cualquier momento que trata los datos personales de forma legal y con respeto. Los programas o metodologías especializadas pueden ser útiles, pero en muchos casos son innecesarios. Las dos columnas mencionadas anteriormente, que usted puede vincular a los registros simples de las operaciones de procesamiento de datos, proporcionarán gran parte de las pruebas que usted necesitará, siempre y cuando la información se introduzca con el debido cuidado.

En el próximo capítulo examinaremos con más detenimiento las áreas en las que se pueden implementar medidas de protección para garantizar que los datos personales se almacenen y procesen de forma segura.

CAPÍTULO 15

Medidas de protección de datos personales

En el anterior capítulo, discutimos la importancia de una evaluación de impacto. El tamaño de cada riesgo determina qué medidas de protección son necesarias. En este tramo se discuten las medidas concretas a tomar. Obviamente, una organización pequeña no se ocupará de estos asuntos de la misma manera que una gran empresa. Dicho esto, una breve introducción al marco de un sistema como ISO 27001 es útil, ya que se debe seguir el mismo razonamiento.

Los primeros aspectos cubiertos por la norma ISO 27001 se refieren a la política y la organización. Debe formular los puntos de partida de su política. Esto se puede hacer en tan sólo dos frases. El uso de los datos personales debe ser legal y tener una finalidad legítima. También debe asegurarse de que los datos estén adecuadamente protegidos. El director general es el responsable de formular la política en este ámbito, y aunque puede delegar esta tarea, sigue siendo responsable y debe evaluar la eficacia de la política cada año.

Los siguientes aspectos se refieren a medidas en diversos ámbitos que deben ser adoptadas de una u otra manera por todas las empresas y organizaciones, independientemente de su naturaleza.

- Empleados (Filtrado / formación y sensibilización / antiguos empleados)
  - Al contratar empleados, preste atención al sentido de responsabilidad de los candidatos.
  - Si usted procesa datos confidenciales, solicite una lista de condenas anteriores (también tendrá que tratar esto como información confidencial).

- Incluya una cláusula de confidencialidad en sus contratos de trabajo. Esto puede adoptar la forma de una simple frase, como por ejemplo: “Todos los datos personales que utilice en su entorno de trabajo son confidenciales y sólo pueden utilizarse para la tarea que debe realizar”.
- Asegúrese de que sus empleados reciban regularmente formación sobre la protección de datos.
- Asegúrese de que los ex-empleados ya no tengan acceso a los datos y no retengan ningún activo de la empresa, incluyendo los datos en papel o en formato digital.

- Clasificación y uso de los activos
  - Mantenga registros de las operaciones de tratamiento de datos y complemente estos registros realizando una evaluación de riesgos.
  - Tenga cuidado con los medios extraíbles, por ejemplo, las memorias extraíbles que contienen datos y los dispositivos que deben desecharse. Tome medidas para evitar que los datos caigan en manos equivocadas.
- Derechos de acceso
  - Asegúrese de que sus contraseñas son lo suficientemente complejas y manténgalas estrictamente privadas.
  - Permita que sus empleados sólo tengan acceso a la información que necesitan para realizar su trabajo. Utilice categorías de trabajo para este propósito.
  - Restrinja los derechos de administrador en los sistemas sólo a personas autorizadas.
- Criptografía
  - El RGPD menciona específicamente el cifrado de datos como una medida de protección, y ciertamente es aconsejable utilizar el cifrado al intercambiar datos o almacenarlos durante largos períodos de tiempo.
  - Algunos ejemplos incluyen el uso del protocolo HTTPS en sitios web, el protocolo SFTP para la transferencia de datos y el cifrado del correo electrónico.
  - Un partner de TIC puede prestar asistencia. No olvide llegar a acuerdos adecuados con su partner de TIC para que no represente un nuevo riesgo de seguridad.
- Seguridad física
  - Encienda el salvapantallas de su PC cuando no esté en su escritorio.
  - No deje ningún documento al final de la jornada laboral (política de limpieza del escritorio).
  - Desarrolle un plan clave para escritorios y armarios.
  - Es posible que necesite puertas, un sistema de alarma, una cámara de vigilancia o un sistema de placas, y quizá, zonas separadas dentro de sus edificios.
  - Proteja su equipo contra cortes de corriente. Tome medidas para prevenir fallas mecánicas.

- Acompañar siempre a los visitantes y proporcionarles pautas de confidencialidad.
- Preste atención adicional a las salas que contienen datos confidenciales, como salas de servidores o archivos donde se almacenan los expedientes confidenciales.

- Seguridad de red
  - Utilice un firewall, protección antivirus y filtrado de contenido para proteger su red contra riesgos externos.
  - Divida las redes más grandes en zonas. Tome medidas para prevenir fallas del sistema. Supervise y registre la actividad de red.
- Medidas de seguridad para el desarrollo de aplicaciones o sistemas
  - Separe el entorno de prueba de la producción y desarrolle reglas para transferir datos.
  - Considere siempre la seguridad y realice pruebas antes de poner en funcionamiento los sistemas.
- Supervisión de las operaciones de tratamiento por terceros
  - Llegue a acuerdos contractuales de seguridad y protección de datos con sus proveedores.
  - Evalúe las operaciones de sus proveedores y haga un seguimiento regular de sus evaluaciones
- Continuidad
  - Asegure el mantenimiento adecuado y la deduplicación para reducir el riesgo de fallas del sistema.
  - Realice copias de seguridad de los datos y elabore un plan de recuperación del sistema para utilizarlo cuando surjan problemas graves.
- Gestión de incidentes
  - Registre todos los incidentes que lo expongan al riesgo de violaciones de privacidad de datos.
  - Cualquier violación de datos que pueda tener un impacto debe ser reportada.
- Auditorías
  - Verifique que su seguridad sea adecuada y hágala evaluar.

Aunque las medidas de esta lista son evidentemente ejemplos, y cada organización gestionará la implementación de una forma ligeramente diferente, puede utilizar la lista para ayudarle a identificar todas las áreas en las que puede reducir activamente los riesgos. En los próximos capítulos se profundizará en algunas de estas áreas, a las que el RGPD presta especial atención. Esto incluye el control de subcontratistas y otros terceros, y lo que se necesita hacer en caso de una vulneración de datos.

CAPÍTULO 16

Gestionar los riesgos asociados a las subcontrataciones y a los acuerdos de procesamiento de datos

Como hemos señalado anteriormente en este blog, pueden surgir riesgos y, por lo tanto, es necesario tomar medidas de seguridad cuando las empresas y organizaciones subcontratan. El RGPD es muy claro en este punto. Aunque los subcontratistas tienen sus propias responsabilidades y una serie de obligaciones, un responsable del tratamiento de los datos que contrata a un subcontratista en el papel de encargado del tratamiento sigue siendo siempre responsable de los datos.

El responsable del tratamiento debe seleccionar cuidadosamente a cada subcontratista y garantizar la ejecución del contrato, debe formular y definir con claridad la tarea pertinente, y verificar que el subcontratista cumple sus instrucciones y la legislación, en particular en materia de seguridad.

En los últimos años ha habido una creciente conciencia entre los especialistas en seguridad de la información de que los subcontratistas siempre representan un riesgo. Por lo tanto, no es sorprendente que el RGPD preste mucha atención a esta cuestión.

En las diferentes fases de una relación de trabajo se deben tomar varias medidas. A la hora de seleccionar proveedores, siempre debe prestarse atención a la protección de datos y a la seguridad de la información. El responsable del tratamiento debe asegurarse de que cualquier subcontratista que se proponga contratar es consciente de sus obligaciones y puede cumplirlas adecuadamente. No existe un sistema de certificación que demuestre que una empresa cumple con el “RGPD”, y no he oído hablar de ningún plan específico

para introducir tal sistema. Dicho esto, los organismos oficiales animan a las asociaciones profesionales a elaborar códigos de conducta que las personas puedan firmar para demostrar que conocen las normas y están dispuestas a seguirlas, y los cuestionarios se utilizan cada vez más en los procedimientos de selección y en la documentación de las licitaciones.

Por supuesto, es posible obtener una certificación en el ámbito de la seguridad de la información, pero las vías de certificación están muy orientadas a grandes organizaciones y no son una propuesta viable para cada empresa u organización. Siempre pregunte a su futuro proveedor sobre su política de seguridad de la información y las medidas aplicables, e incluya ambos aspectos en sus criterios de selección. Por último, lleve un registro de la documentación que haya reunido.

Al asignar una tarea, es esencial que tenga algunas cláusulas contractuales sobre protección de datos. La mejor manera de hacerlo es mediante un acuerdo de tratamiento de datos. Esto puede ser un apéndice de otro contrato o acuerdo marco. Algunas cláusulas generales también pueden ser incorporadas en sus condiciones generales, por supuesto. Incluso si usted ha estado trabajando con un subcontratista durante mucho tiempo, todavía necesita asegurarse de que el subcontratista cumple con el RGPD. Dadas las diferencias entre el RGPD y la legislación anterior, que hacía menos hincapié en las obligaciones del procesador, es aconsejable elaborar una versión modificada de su acuerdo de tratamiento de datos.

Todos estos acuerdos de tratamiento de datos deben incluir las siguientes cláusulas:

- Al director se le asigna la función de controlador o responsable del tratamiento, y al contratista/proveedor/subcontratista se le asigna la función de procesador o encargado del tratamiento.
- El encargado del tratamiento sólo podrá utilizar los datos con arreglo a las instrucciones formales (preferentemente escritas) del responsable del tratamiento.
- El encargado del tratamiento respeta la confidencialidad de los datos y también impone esta obligación a todo su personal temporal y permanente.
- El encargado del tratamiento debe ofrecer un nivel adecuado de protección de datos y garantizar que los datos estén y sigan estando disponibles para la tarea, utilizando copias de seguridad y medidas para garantizar la continuidad.
- El responsable del tratamiento debe ser informado inmediatamente en caso de violación de los datos, y debe existir un procedimiento para limitar el impacto de la violación. El encargado del tratamiento no podrá facilitar ninguna información a la AEPD o a los interesados.
- El encargado del tratamiento debe eliminar los datos una vez finalizada la tarea o el período de conservación acordado y también debe poder demostrar que lo ha hecho. En su caso, también deberá devolver los datos al responsable del tratamiento.
- Los datos no deben ser cedidos a terceros salvo que el responsable del tratamiento haya dado su consentimiento. Si el encargado del tratamiento contrata a un

subcontratista con la aprobación del responsable del tratamiento, debe asegurarse de que el subcontratista acepta las mismas obligaciones que las establecidas en el acuerdo de tratamiento de datos.

- El encargado permite al responsable supervisar la correcta ejecución del contrato mediante evaluaciones o auditorías.

Como organización más pequeña, podría beneficiarse del trabajo realizado por sus proveedores más grandes, que probablemente ya han redactado sus propios contratos estándar de encargado de tratamiento para presentarlos a sus clientes.

Por último, el responsable del tratamiento también tiene que comprobar si el encargado cumple correctamente el contrato. En el caso de los contratos a más largo plazo, deberá comprobarlo de forma regular. A este respecto, es esencial que los acuerdos contractuales incluyan el derecho a realizar auditorías. Por supuesto, esto no significa que los responsables tengan que auditar a todos los subcontratistas cada año.

Las grandes organizaciones llevan a cabo estas auditorías (a menudo con gran molestia para sus proveedores), en aquellos encargados de tratamiento que consideran que representan un alto riesgo de una vulneración de datos personales o en los casos en que esta violación tendría un impacto importante. En muchos casos, basta con comprobar si la certificación del proveedor se renueva cada año. Alternativamente, puede pedir al proveedor encargado del tratamiento que rellene y firme un cuestionario en el que se resumen las medidas adoptadas por dicho proveedor.

Como en todos los aspectos de esta legislación, las acciones a tomar deben ser ponderadas contra la probabilidad de que ocurra un incidente y el impacto potencial que esto tendría.

CAPÍTULO 17

Lo que necesita hacer en caso de una violación de datos - Gestión de incidentes

En las anteriores entregas de esta guía explicamos cómo puede tomar las medidas oportunas para garantizar la correcta protección de los datos personales que procesa. Hay que comprender los riesgos potenciales, hay que tomar diversas medidas para reducirlos o eliminarlos si es posible, y si se contrata a subcontratistas, hay que asegurarse de que éstos organizan los trabajos tan bien como usted. Sin embargo, las cosas pueden ir mal. Esta entrega examina lo que debe hacer en tales situaciones.

Una violación de datos es una situación en la que los datos confidenciales se pierden, se modifican erróneamente, se hacen públicos o caen en las manos equivocadas. El RGPD exige que el responsable del tratamiento de datos personales informe a la autoridad de protección de datos de cualquier vulneración de los datos que pueda constituir una violación de la intimidad de los interesados sin demora innecesaria. Si existe un riesgo grave de daños y perjuicios, también habrá que informar a los interesados.

Antes de considerar si una vulneración de datos tiene que ser reportada a la AEPD (Agencia Española de Protección de Datos) , primero hay que centrarse en la gestión de incidentes. Después de todo, su obligación principal como responsable del tratamiento o responsable del tratamiento de los datos es prevenir incidentes y minimizar el impacto de cualquier incidente que se produzca.

En primer lugar, hay que detectar los incidentes lo antes posible. Existen muchas herramientas de red que pueden revelar un comportamiento anormal en la red, detectar

virus o malware, o aplicar el filtrado de contenidos, que puede utilizar para este fin. Dicho esto, los empleados también son capaces de detectar infracciones. Por lo tanto, es crucial que se organicen periódicamente campañas de formación o sensibilización del personal para garantizar que todos sepan claramente qué constituye una situación anormal o preocupante. También es importante que todos los empleados sepan a quién deben llamar cuando ocurre un incidente.

Segundo, debe tomar medidas lo antes posible para poner fin al incidente o limitar su impacto. Todos los empleados tienen que cumplir una serie de reglas. Si se encuentran con información en un lugar donde no pertenece, tienen que borrarla o notificar a alguien responsable. Esta información puede encontrarse en soportes físicos o en archivos ubicados en la red. Si se encuentran con personas extrañas sin compañía en una zona segura, tienen que dar la alarma, y así sucesivamente. Cuando las alertas de monitorización apuntan a la piratería informática o a un sistema infectado, los ingenieros del sistema tendrán que examinar el sistema lo antes posible y quizás tengan que apagarlo como medida preventiva.

En caso de duda, es mejor detener las operaciones de tratamiento y bloquear las transferencias de datos procesados hasta que se tenga la certeza de que existe un problema y se conozca el grado de afectación de los datos procesados. Al hacer esto, a menudo puede asegurarse de que un incidente no se convierta finalmente en una violación de datos. Mientras no se difundan o divulguen datos tratados incorrectamente, no se considera que se ha producido ninguna infracción y, por lo tanto, no hay ningún impacto que tratar. En ese caso, estrictamente hablando, no hay violación de datos.

A continuación, se puede iniciar un análisis de los hechos, si es necesario en paralelo con lo anterior. Esto establecerá la verdadera causa del problema. A continuación, se puede pensar en introducir mejoras en la organización, los sistemas, las aplicaciones y la forma de trabajar de los empleados para evitar que se repitan. El análisis también considerará el impacto potencial o real, si la confidencialidad e integridad de los datos está en peligro, si alguno de los datos son datos personales y las posibles consecuencias de la infracción. En muchos casos, el establecimiento de la cantidad de datos y, por lo tanto, del número de personas afectadas por el incidente llevará algún tiempo. Por otra parte, no siempre está claro si existe un riesgo real de impacto y, en particular, el alcance potencial del daño.

Usted debe poder responder a las preguntas anteriores antes de decidir si la vulneración de datos debe ser comunicada a la AEPD o a los interesados. Si usted necesita hacer esto, y, si es así, cuándo, será el tema del próximo capítulo.

Además, todos los incidentes deben registrarse en sus registros internos. Todos los incidentes deben ser analizados tanto las brechas de datos reales, como los fallos que han quedado cerca. La información resultante es crucial para evaluar los procedimientos y directrices existentes y comprobar si las medidas adoptadas ofrecen una protección adecuada contra los posibles riesgos. Deben registrarse las causas de un siniestro, así como las acciones correctoras previstas. El seguimiento de incidentes según un plan fijo mejorará sistemáticamente la seguridad de su organización.

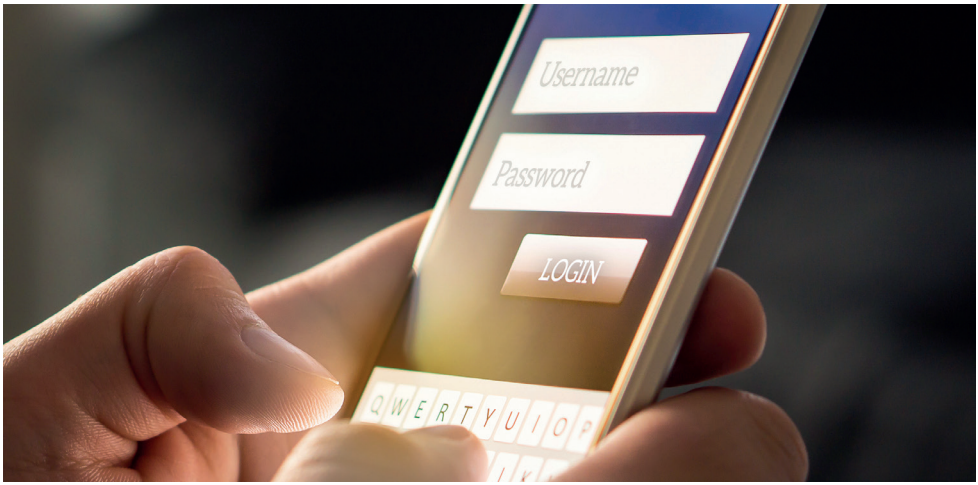
En casos extremos, una violación de datos puede tener consecuencias desastrosas. Una organización puede enfrentarse a enormes problemas de comunicación si se filtra

información altamente sensible sobre un gran número de base de datos. En algunos casos, la violación de los datos es conocida por personas ajenas a la organización y la prensa ya lo sabe. En tales situaciones, es útil poder recurrir a escenarios de comunicación de crisis ya preparados. Si su organización ha contratado un seguro de seguridad cibernética, es posible que su asegurador pueda ayudarle con esto.

Cuando existan sospechas de que se han cometido delitos penales, también debe asegurarse de que se compila rápidamente un archivo legal. A veces es necesario hacer una copia de seguridad rápida de la situación en el momento en que se descubrió el incidente, o sacar en paralelo archivos “log”, antes de que los datos pertinentes desaparezcan o sean cambiados por las medidas adoptadas para resolver el incidente.

Obviamente, esto a veces significará ir en contra de lo que hay que hacer para limitar rápidamente el problema existente. Si la policía o los tribunales están involucrados, tampoco debe perder de vista lo que puede y no puede hacer cuando actúa bajo su propia autoridad, especialmente si su función es la de encargado de tratamiento o procesador. En ese caso, es necesario involucrar al controlador o responsable del tratamiento lo antes posible. Si las autoridades le exigen que entregue información, seguirá estando bajo la obligación ante el responsable del tratamiento de proteger esta información en la medida de lo posible, y debe asegurarse de que no divulgue ningún dato que no sea necesario para los fines de la investigación.

Estos pasos deben estar bien documentados para que todos los miembros de la organización los conozcan y actúen en consecuencia. También le ayudará a demostrar que se toma en serio sus obligaciones en virtud del RGPD.



CAPÍTULO 18

Lo que debe hacer en caso de violación de los datos - Obligación de notificación

Como ya explicamos en el anterior capítulo, una vez que se ha detectado una vulneración de datos, la primera preocupación es minimizar el impacto. Además, el Reglamento sobre protección de datos personales exige que el responsable del tratamiento notifique a la autoridad encargada de la protección de datos, sin demora injustificada, cada vulneración de los datos que probablemente entrañe un riesgo de violación de la intimidad. Deberá informarse también al interesado si es probable que este riesgo sea grave.

Esta obligación plantea muchas preguntas. ¿Cuándo un incidente de seguridad de la información se convierte en una violación real de los datos? ¿Cuándo una violación de los datos supone un riesgo de violación de la privacidad? ¿Cuándo existe un riesgo grave de daños? ¿En qué momento se da cuenta del incidente y tiene la obligación de denunciarlo?

En caso de que el incidente implique datos personales, deberá en cualquier caso informar a su responsable de protección de datos (DPO). Si no tiene un DPO oficial, es esencial que alguien asuma esta función. El responsable de la protección de datos está en la mejor posición para determinar la importancia de los datos y la gravedad del impacto potencial de una infracción para los interesados y para el responsable del tratamiento, ya sea su propia organización o, si usted es un responsable encargado por otra parte, su cliente. El DPO asesora a la organización sobre la comunicación necesaria. También es la persona más indicada para decidir si se debe notificar a la AEPD y qué información se puede proporcionar directamente.

Simplemente, puede hacerse tres preguntas para determinar si la notificación es necesaria:

- ¿Ha habido efectivamente una violación de datos? Si una situación podía dar lugar a una violación de los datos, pero no se revelaron o cayeron en las manos equivocadas, no se considera que vaya más allá de un incidente. Por lo tanto, debe registrarlo en su "log" interno, pero no es necesario el aviso.
- ¿El incidente probablemente no implica ningún riesgo? Incluso si los datos terminan fuera de las zonas seguras o fuera de su organización, es posible que no exista un riesgo real debido a las medidas de protección adoptadas. Por ejemplo, los datos pueden haberse cifrado de tal manera que no puedan ser utilizados por terceros.
- ¿Existe un grave riesgo inmediato de daños a los interesados? Si se produce una vulneración de los datos relativos a los datos de la tarjeta de crédito, por ejemplo, existe el riesgo de que se produzcan daños económicos y los interesados deben ser informados lo antes posible para que puedan tomar medidas por sí mismos. Este puede ser también el caso si la violación de los datos involucra varios tipos de información sensible. Si los datos en cuestión son triviales, informar a todos es un asunto menos urgente. El RGPD también prevé situaciones en las que es casi imposible notificar a todos los interesados por separado. En tales casos, las comunicaciones públicas también se consideran adecuadas.

El RGPD también establece normas que especifican la información que debe incluirse en la notificación:

- Una descripción de la infracción, indicando, en la medida de lo posible, el tipo de los interesados afectados y las categorías de datos.
- El número aproximado de interesados, cuando sea posible.
- Los datos de contacto de su DPO o del punto de contacto para cuestiones de privacidad de datos.
- Impacto probable de la infracción.
- Las medidas adoptadas por el equipo encargado del siniestro para limitar el impacto.

Es posible que parte de esta información no esté disponible de inmediato y que sea necesario un análisis más profundo para establecer algunos de los hechos. Por lo tanto, el RGPD especifica que la notificación debe efectuarse "sin retrasos indebidos" y no "inmediatamente". La norma consiste en notificar a la autoridad supervisora a más tardar setenta y dos horas después de que el responsable del tratamiento tenga conocimiento de la violación de los datos. La notificación también puede demorarse más de setenta y dos horas, siempre que se dé una explicación razonable. Parte de la información sobre la infracción también podrá facilitarse con posterioridad a la notificación inicial.

Si usted actúa en calidad de procesador o encargado del tratamiento, y no de controlador o responsable, debe tener especial cuidado cuando se produce una violación de datos. Esto se debe a que usted corre el riesgo de salirse de los límites de su propia área de responsabilidad y, como resultado, estar cada vez más expuesto a responsabilidad. Por lo tanto, la mayoría de los acuerdos del procesador de datos establecen claramente que

si el procesador detecta una violación de los datos, debe ponerse en contacto con el responsable del tratamiento inmediatamente y nunca debe comunicarse con la AEPD o con los propios interesados.

La mejor forma de comunicarse con la prensa es también dejarla en manos del controlador. A diferencia de los controladores, que por ley tienen hasta setenta y dos horas para notificar al supervisor (AEPD) en circunstancias normales, se espera que los procesadores informen al controlador inmediatamente si detectan una infracción. Esto permite al controlador empezar a desempeñar su función directamente. Los contratos a menudo requieren que el procesador responda dentro de veinticuatro horas, aunque la ley establece setenta y dos horas.

Decidir qué comunicaciones y qué notificaciones son necesarias no siempre será sencillo. La falta de notificación de una violación de los datos es un delito y expone al responsable del tratamiento a multas potencialmente muy elevadas. Al mismo tiempo, la lista de violaciones de datos es una información pública. Ninguna empresa desea ser incluida en esta lista, sobre todo si posteriormente se descubre que no se ha producido ninguna violación de datos o si los datos están tan bien protegidos que no hay riesgo de daños. Su imagen puede sufrir mucho antes de que esto salga a la luz.

Por el contrario, ninguna empresa quiere tener la reputación de tratar de encubrir problemas graves. A este respecto, la apertura y la transparencia son siempre la mejor política. Las autoridades podrían emitir directrices adicionales para aclarar cuándo la notificación es apropiada y cuándo no lo es. Los especialistas en privacidad también advierten del peligro de que, en un esfuerzo por evitar multas, las empresas puedan informar sobre incidentes periféricos demasiado pronto, saturando a las autoridades con notificaciones de siniestros que éstas no pueden verificar y procesar.

Es recomendable que, de todos modos, todos los incidentes se identifiquen en el registro interno de incidentes, que debe mantenerse con arreglo a las disposiciones del RGPD, detallando los hechos establecidos, el impacto y las medidas correctoras que se han tomado. También puede documentar su línea de razonamiento para no notificar el incidente o no informar a los interesados, por ejemplo. Esto le permitirá demostrar en una fase posterior que se ha detectado un incidente y que se han tomado las medidas adecuadas. El seguimiento de incidentes de esta manera también contribuye en gran medida a mejorar los procedimientos y las medidas de protección.

CAPÍTULO 19

Los derechos del interesado - El derecho a ser informado

En pasadas entregas de esta guía tratamos principalmente sobre las obligaciones que el RGPD impone a las empresas y organizaciones que procesan datos personales. Hemos considerado la legislación principalmente desde el punto de vista de los controladores o responsables del tratamiento y de los procesadores o encargados del tratamiento de datos personales. Ha llegado el momento de centrarnos en los distintos interesados.

Uno de los principales objetivos del RGPD es especificar sus derechos como individuo con respecto a la gran cantidad de datos circulantes que le conciernen y son utilizados por otros. Como titular de los datos, usted puede acceder a esta información, aunque sus derechos no sean absolutos, como veremos a continuación.

Uno de los conceptos más importantes del RGPD es la transparencia. Todo encargado de tratamiento de datos personales debe esforzarse por ser abierto con las personas o interesados a las que se refieren los datos. Debe ser fácil para los interesados saber qué datos son conservados y tratados por el encargado del tratamiento, qué hace el encargado del tratamiento con los datos y por qué son necesarias estas operaciones de tratamiento. El encargado del tratamiento debe ser capaz de explicar esto en un lenguaje claro y sencillo. Los capítulos once y doce contienen una consideración detallada de cómo las empresas y organizaciones pueden proporcionar esta información en forma de declaración de privacidad en sus sitios web.

El encargado del tratamiento debe asegurarse de que usted, como titular de los datos, está debidamente informado con antelación de sus intenciones, las posibles consecuencias y

los riesgos a los que está expuesto, especialmente si se solicitan datos que se pretende conservar y utilizar. Debe explicar también cómo los beneficios de esto superan las desventajas.

Adicionalmente, el responsable del tratamiento debe indicar lo que usted puede hacer si tiene una pregunta o queja. Debe contar con un punto de contacto directo dentro de la organización. Además, el encargado del tratamiento debe informarle de que puede presentar una reclamación sobre una operación de tratamiento ante la autoridad responsable del tratamiento. Obviamente, si usted presenta una queja debe tener un motivo válido para ello.

Además del derecho a la información general, como titular de los datos también tiene derechos específicos en lo que se refiere a sus propios datos personales. Cualquier persona podrá dirigirse a un responsable del tratamiento para acceder a los datos personales que la empresa u organización conserve en él y obtener información sobre las operaciones de tratamiento para las que se utilizan los datos. Tales peticiones “simples” pueden crear mucho trabajo para la empresa u organización. Poder responder con precisión a estas solicitudes significa estar bien preparado y seguir un procedimiento claro, sobre todo porque en el marco del RGPD los interesados tienen derecho a recibir una respuesta en el plazo de un mes. El responsable del tratamiento deberá facilitar la información solicitada dentro de ese plazo o bien explicar por qué necesita más tiempo.

Hay varios escollos importantes que hay que superar para cumplir esta obligación. Primero, el responsable del tratamiento debe saber dónde se puede encontrar la información. Esto no es un problema cuando se trata de archivos con detalles de contacto en una aplicación CRM o datos de personal almacenados en un sistema administrativo. Desafortunadamente, gran parte de la información se almacena como datos no estructurados en archivos de papel, en archivos digitales que no están cubiertos por el sistema de gestión de documentos, o a nivel local por empleados individuales. La recopilación de estos datos es mucho más difícil. Además, el RGPD establece explícitamente que este servicio debe ser gratuito, salvo en los casos en que las solicitudes recibidas sean manifiestamente infundadas o excesivas.

Dicho esto, este derecho de acceso entra en conflicto con otros derechos e intereses. Al proporcionar información a un interesado, el responsable del tratamiento debe asegurarse, por ejemplo, de que no infringe los derechos de otros interesados. Por ejemplo, será prácticamente imposible que una empresa u organización acepte inmediatamente la solicitud de acceso a todos los documentos y correos electrónicos en los que se mencione a una persona. Esto se debe a que tales documentos incluyen información sobre otras personas, cuya privacidad también debe protegerse. Algunas fuentes de información también contienen otros datos confidenciales, que podrían dañar los intereses de la empresa si se divulgan. En todas estas situaciones, será necesario ponderar los diferentes derechos y alcanzar un punto de vista equilibrado. El resultado puede ser que no se pueda cumplir con la solicitud del interesado. En tal caso, el interesado debe ser informado del motivo.

Además del derecho a ser informados, los interesados tienen muchos otros derechos en virtud del RGPD, éstos serán discutidos en la próxima entrega.

CAPÍTULO 20

Derechos del interesado - Derechos relativos a los propios datos

En el anterior capítulo, discutimos el derecho del interesado a ser informado. Todo responsable del tratamiento debe proporcionar información transparente sobre el tipo de datos que conserva, las operaciones de tratamiento para las que se utilizan los datos y la finalidad de dichas operaciones. Además, cada interesado tiene derecho a acceder a sus propios datos.

Sin embargo, los derechos del interesado y, por lo tanto, las obligaciones impuestas al responsable del tratamiento, van mucho más allá. El interesado también puede solicitar que rectifique, complemente o incluso borre los datos que conserve sobre él o ella. El derecho del interesado a que se eliminen los datos no es absoluto, y las posibilidades de cumplir con esta petición deben sopesarse con otros derechos y obligaciones legales. Cuando existe una obligación legal de archivar los datos durante un período de tiempo determinado, es evidente que los datos no pueden suprimirse a petición de una sola persona. A veces, los datos deben conservarse durante un tiempo para que puedan cumplirse todas las obligaciones contractuales. Además, los responsables del tratamiento de datos tienen que conservar una cantidad limitada de datos para poder documentar su conformidad con las solicitudes de los interesados para la eliminación de datos.

Sobra decir que el derecho de rectificación también es relativo. Obviamente, un informe de evaluación archivado de un empleado no se puede modificar simplemente porque el empleado lo solicite. En tales situaciones, los empleados pueden ejercer sus derechos añadiendo comentarios. Por ejemplo, las rectificaciones de datos, incluso pueden ser útiles,

cuando los datos se obtienen a través de terceros. Sin embargo, las cosas se complican mucho más desde el punto de vista jurídico, cuando se trata del enriquecimiento de los datos por parte del responsable del tratamiento, que podría constituir el valor añadido que incorpora el responsable del tratamiento.

Por regla general, cualquier solicitud de modificación o eliminación de datos es también aplicable a todos los terceros a los que se transmitieron los datos, como socios o subcontratistas. El responsable del tratamiento debe garantizar que los terceros sean informados de dichas solicitudes siempre que sea posible. El conocido derecho al olvido ya ha sido objeto de una serie de procedimientos judiciales de alto nivel relacionados con los medios de comunicación social. Es evidente que el cumplimiento exhaustivo de este tipo de solicitudes no es en absoluto sencillo. En vista de ello, los contratos celebrados entre los responsables del tratamiento y sus subcontratistas deberían especificar que los datos deben suprimirse inmediatamente después del tratamiento.

El interesado también podrá solicitar que se detenga o suspenda el tratamiento posterior de sus datos aunque se conserven. Este enfoque puede ser adecuado en caso de que se produzca una reclamación en curso que esté a la espera de una decisión de las autoridades competentes, por ejemplo, porque el interesado haya impugnado la legalidad de la operación de tratamiento. Evidentemente, una solicitud de este tipo no puede cumplirse si la operación de tratamiento correspondiente se realiza sobre la base de una obligación legal o como parte de las obligaciones del gobierno. Como ya se ha comentado en un apartado anterior, el tratamiento realizado sobre la base del consentimiento prestado por el interesado podrá ser interrumpido en cualquier momento si éste retira su consentimiento. En ese caso, el responsable del tratamiento también debe borrar los datos.

Por último, el interesado también tiene derecho a la portabilidad de los datos. Este derecho ya estaba incluido en la legislación sobre privacidad electrónica, que impone obligaciones a los proveedores de servicios digitales. El objetivo subyacente de este derecho era impedir que los clientes que quisieran cambiar de proveedor de servicios fueran “rehenes” de su proveedor de servicios actual debido al hecho de que perderían todos sus datos. Después de todo, nadie quiere perder todas las fotos, blogs y correos electrónicos que se almacenan en línea.

El mismo derecho se ha incluido ahora también en el RGPD y es aplicable a todas las operaciones de tratamiento de datos personales. En este contexto mucho más amplio, la portabilidad de los datos a menudo no es factible en la práctica. Además, genera conflictos con otros derechos. Por ejemplo, un responsable de tratamiento que ha realizado operaciones complejas sobre datos (algunos de los cuales pueden estar basados en algoritmos que son propiedad intelectual de la empresa), no querrá revelar esos resultados sin una buena razón. Por lo tanto, la interpretación más comúnmente aceptada es que el derecho a la portabilidad de los datos sólo es realmente aplicable en el caso de los datos que el interesado puso a disposición del encargado del tratamiento.

Se aconseja a las organizaciones que establezcan un procedimiento adecuado para tratar todas estas solicitudes.

- En primer lugar, el punto de contacto para cualquier pregunta, así como la persona responsable dentro de la organización, debe quedar claro a los interesados. Esta

información puede incluirse en una declaración de privacidad, por ejemplo.

- Dentro de la organización, las solicitudes deben transmitirse rápidamente a la persona adecuada para su posterior tramitación, lo que significa que todos deben conocer el procedimiento.
- Debe existir un método claramente definido para determinar si la identidad de la persona que presenta la solicitud es la misma que la del interesado cuyos datos se solicitan. Por lo general, se recomienda que la organización pida a la persona solicitante que presente una fotocopia de su documento de identidad.
- También es preciso establecer normas para determinar no sólo qué información puede facilitarse, sino también, en su caso, qué información no puede facilitarse, por ejemplo, ¿podríamos incluir datos confidenciales sobre otras personas o secretos comerciales? Deben documentarse las líneas de razonamiento que deben seguirse. En este contexto, los derechos de todas las personas afectadas deben tratarse de manera equilibrada, ya que los derechos del interesado no son absolutos.
- Un sistema de seguimiento debe garantizar que todas las solicitudes se tramiten con prontitud y que se conserve la documentación relativa a los progresos realizados y las decisiones adoptadas.

Es evidente que el ejercicio de estos derechos planteará problemas prácticos a los responsables del tratamiento de datos. En algunos círculos también existe la preocupación de que los activistas de la privacidad de datos utilicen la ley para atacar a las empresas bombardeándolas con peticiones organizadas en masa. Sin embargo, el RGPD ofrece una cierta protección contra esto al especificar que las solicitudes no deben ser infundadas o excesivas (por ejemplo, porque las solicitudes se hacen repetidamente). Los encargados del tratamiento no están obligados a cumplir con ninguna solicitud que pueda resultar infundada o excesiva.

A pesar de lo anterior, el hecho de que nosotros, como individuos, seguiremos teniendo, al menos hasta cierto punto, el control de la información que existe sobre nosotros y que las empresas y organizaciones dispongan de un marco para el tratamiento respetuoso y cuidadoso de los datos personales es, por supuesto, un hecho que debe acogerse con satisfacción.

CAPÍTULO 21

Responsabilidad bajo el RGPD

Ahora que hemos cubierto todo lo esencial sobre el RGPD, quedan algunas cuestiones que se deben considerar a un nivel más global. Una de ellas es la responsabilidad de los procesadores y controladores. Todas las personas que procesan datos personales deben cumplir con los requisitos establecidos en el RGPD, y también deben ser capaces de demostrar y probar que se han cumplido dichos requisitos. Si está familiarizado con las auditorías, sabrá lo que esto implica. Una vez que haya explicado por qué medios garantiza el cumplimiento de las obligaciones específicas, también debe demostrar que realmente sigue los procedimientos pertinentes y que supervisa adecuadamente cómo los llevan a cabo sus empleados. Este es el tema de esta entrada del blog.

Una gran cantidad de trabajo administrativo consiste en demostrar que usted está familiarizado y entiende todos los aspectos del RGPD, y que su propia organización cumple con los requisitos. La aplicación debe ser pragmática pero exhaustiva, especialmente en las pequeñas empresas, organizaciones y asociaciones. Puede encontrar muchos consejos sobre cómo hacer esto en los anteriores posts. En el futuro, tendrá que mantener su documentación actualizada.

En primer lugar, debe asegurarse de que su organización dispone de conocimientos suficientes. En las organizaciones que cuentan con un Responsable de Protección de Datos (Data Protection Officer o DPO), la responsabilidad se confía al DPO y a su personal. Incluso si usted no tiene un DPO, necesita estar bien informado y proporcionar formación a sus empleados.

Los registros de las operaciones de tratamiento de datos personales son fundamentales para demostrar el cumplimiento. Está obligado a mantener estos registros bajo el RGPD, que al mismo tiempo suponen un punto de partida ideal para documentar cómo asegurar la protección de datos. Para cada operación de tratamiento que se describe, debe demostrar que ha pensado en la finalidad y el fundamento jurídico de la operación de tratamiento, que ha sopesado el riesgo de una violación de datos y que ha tomado todas las medidas de seguridad apropiadas. Por supuesto, también es necesario desarrollar un procedimiento adecuado para garantizar que esta información permanezca completa. Cada operación de tratamiento adicional debe introducirse en los registros. El DPO tiene un papel importante que desempeñar en este sentido. Él o ella brinda asistencia y supervisa si el procedimiento se realiza de manera precisa y oportuna.

En el caso de proyectos importantes, este examen preliminar puede formalizarse aún más en forma de una Evaluación de Impacto de la Protección de Datos (Data Protection Impact Assessment o DPIA). Se trata de un análisis formal de una operación de tratamiento de datos cuyo objetivo es identificar todos los riesgos potenciales de violación de la intimidad, enumerar todas las medidas de protección y determinar si la finalidad y el fundamento jurídico de la operación de tratamiento cubren los riesgos restantes. Si una operación de tratamiento intensivo implica categorías especiales de datos personales, debe presentarse un DPIA a la autoridad de protección de datos (DPA – en Bélgica esta es la Comisión de Privacidad).

Por supuesto, todas las medidas adoptadas en el ámbito de la seguridad también deben estar debidamente documentadas. Cuando se lleva a cabo una auditoría de protección de datos, se espera que pueda demostrar inmediatamente qué procedimientos son aplicables, de cuándo es la versión más reciente, los empleados que aplican cada procedimiento, y si estos empleados han sido notificados y saben qué hacer. Si alguno de los procedimientos incluye verificaciones periódicas, es importante establecer de una forma u otra que estas verificaciones se realicen realmente. Es mejor mantener los archivos de registro técnicos y los informes de supervisión durante algún tiempo. Si se llevan a cabo verificaciones manuales, es necesario crear un informe breve o actualizar un registro, por ejemplo, para poder mostrar cuándo se realizaron estas verificaciones y quién las realizó. Además, todo el sistema de seguridad debe evaluarse periódicamente (al menos una vez al año) y ajustarse para reflejar los cambios en la organización, las herramientas y técnicas utilizadas o las soluciones de seguridad disponibles.

En este contexto, debe prestar especial atención al registro de incidentes y brechas de datos. Toda situación que entre en conflicto con los procedimientos normales de seguridad y todo hallazgo que exponga la existencia del riesgo de una violación de datos, debe registrarse con precisión en un registro de incidentes. Obviamente, los ítems indicados en este registro necesitan ser investigados con mayor detalle para determinar su causa subyacente. Al mismo tiempo, se planifican acciones con el objetivo de reducir el riesgo. Algunos ejemplos de medidas que pueden adoptarse son las medidas técnicas de seguridad adicionales, los procedimientos y controles adicionales o modificados, y las nuevas formas de notificación o registro. Esto necesita ser documentado para que usted pueda demostrar su responsabilidad. Si bien no se requiere necesariamente un sistema de monitorización complejo para este propósito, al menos debe tener varios registros bien organizados que

contengan información sobre todos los incidentes (incluyendo su análisis y las soluciones acordadas), así como todos los elementos de acción, su estado y la persona a la que se le ha asignado la responsabilidad.

Se debe prestar especial atención a los acuerdos contractuales con socios o proveedores. Es necesario cerrar acuerdos de tratamiento de datos con subcontratistas para asegurarse de que también cumplen adecuadamente con la legislación. Es una buena idea mantener registros de los subcontratistas a los que se han confiado sus operaciones de procesamiento de datos personales, en los que especifique con precisión lo que cada subcontratista ha tenido que hacer y cómo ha llegado a un acuerdo al respecto. Esto puede enlazarse a un contrato específico. Además, debe asegurarse de que su propia casa está en orden si usted es un procesador que actúa para un cliente. Las operaciones de tratamiento deben introducirse en sus registros, aunque como responsable no es necesario que introduzca tantos detalles como el responsable del tratamiento. También en este caso es esencial que todos los acuerdos cruciales se incluyan en un acuerdo de tratamiento de datos.

Por último, debe poder demostrar que es capaz de garantizar los derechos de los interesados. Debe establecer un acuerdo adecuado sobre el procedimiento que debe seguirse en caso de que un interesado formule preguntas. Es mejor mantener registros de algún tipo de todas las actividades que usted realiza en este contexto. Si usted mantiene registros de cada solicitud recibida de un individuo, anotando la fecha y hora en que fue recibida y todas las acciones tomadas posteriormente, podrá monitorizar si ha reaccionado a tiempo y si ha respondido adecuadamente. También significa que siempre podrá demostrar que cumple con la legislación de la mejor manera posible si es auditado por la DPA o en caso de una queja. Mantener un registro de la línea de razonamiento que se siguió es crucial, particularmente si usted no está dispuesto o no puede cumplir con la solicitud.

Por lo tanto, el simple cumplimiento de la legislación no es suficiente. También tiene que documentarlo y ser capaz de probarlo. Por último, es crucial que se tomen medidas previas al comienzo de todos los proyectos futuros para minimizar los riesgos potenciales. Éste será el tema de la próxima entrega de este blog.

CAPÍTULO 22

El futuro del RGPD: el diseño de la privacidad

A medida que llegamos al final de nuestro largo viaje por el mundo de la protección de datos, tenemos que considerar un aspecto final: la privacidad desde el punto de vista del diseño. La legislación quiere que todos los responsables del tratamiento de datos tengan en cuenta el derecho a la privacidad a la hora de planificar las operaciones de tratamiento de datos personales en el futuro.

De ese modo, los creadores del RGPD asumen que esa gestión de la privacidad se refleje en lo que hagamos. Si lo hacemos, los requisitos legales se convertirán en un aspecto natural y evidente en la construcción de una aplicación o en la configuración de un sitio web o, igualmente, en la organización de una encuesta o de la realización de un estudio científico.

Es mejor no recopilar o procesar datos personales excepto cuando sea necesario; e incluso cuando tenemos una buena razón para recopilar y procesar tales datos, necesitamos limitar las operaciones de procesamiento a las estrictamente necesarias. Por lo tanto, todas las nuevas iniciativas en esta materia requieren una reflexión sobre qué es lo que debemos hacer.

- Aunque en el pasado se consideraba aconsejable añadir más atributos o campos a un fichero al realizar un análisis para una nueva aplicación o al diseñar una base de datos (partiendo de la idea de que podrían resultar útiles en el futuro), hoy en día es más importante que la cantidad de datos se reduzca al mínimo y se adapte a la finalidad específica para la que se procesarán los datos.

- Es aconsejable incluir información en una base de datos para indicar cuándo un dato específico está desactualizado u obsoleto, o simplemente cuándo debemos dejar de conservarlo. Esto facilita la eliminación sistemática de datos cuando ya no son necesarios, o cuando ya no podemos garantizar la exactitud de los mismos.

En el futuro, las solicitudes deberían contener una funcionalidad que garantice los derechos del interesado y facilite su ejercicio en la práctica.

- Siempre que en una solicitud se pidan datos personales a los interesados, debemos facilitar al mismo tiempo información sobre la finalidad para la que se solicitan, la duración del tratamiento de esos datos, los riesgos que entraña y las medidas de protección. Por ejemplo, una aplicación para el smartphone que registra el rendimiento deportivo debe proporcionar al usuario información adecuada sobre los datos que recopila y almacena en segundo plano, y comunicar qué pretende hacer su creador con esos datos antes de que el usuario utilice la aplicación por primera vez. Es conveniente que se incorpore este aspecto en las interfaces de usuario de las aplicaciones.
- Del mismo modo, todo aquel que intente recopilar datos a través de un sitio web debe ofrecer inmediatamente información básica y clara sobre las operaciones de tratamiento de datos. Dicha información debe proporcionarse en el momento oportuno. Además, en la medida de lo posible, se deben establecer distinciones entre los diferentes propósitos potenciales.
- Las futuras aplicaciones también podrían incluir una funcionalidad que permita a los interesados visualizar sus datos y, si la situación lo permite, rectificarlos, completarlos o suprimirlos. Por supuesto, esto sólo es posible si los derechos del interesado no entran en conflicto con otros intereses.

La privacidad por diseño también significa que, cuando se diseña una aplicación, se consideren desde el principio las mejores prácticas para proteger los datos.

- Por ejemplo, siempre que sea posible, puede crear la aplicación de manera que todo esté cifrado. Una web puede utilizar protocolos de cifrado, como puede ser https, y los datos pueden intercambiarse mediante archivos cifrados enviados a través de canales también cifrados. Si los datos deben conservarse durante algún tiempo después de una operación de tratamiento, también pueden conservarse en un archivo cifrado, por ejemplo, en un archivo digital seguro. Todas estas medidas reducen el riesgo de que los datos se hagan públicos o caigan en las manos equivocadas. Es importante tomar estas medidas desde el comienzo de la fase de diseño, ya que, además, será más barato que hacer los cambios más adelante.
- Otra medida que también puede considerarse en algunas circunstancias es la seudonimización de los datos. Esto significa que eliminamos las referencias directas a individuos específicos de los archivos. A través de esta medida se reduce el riesgo de infracciones en caso de que se produzca un percance en relación con un expediente.

Todo esto nos lleva a hablar de la privacidad por defecto; lo que significa que cuando una aplicación permite al usuario elegir entre hacer públicos o no los datos, compartirlos con otros o ponerlos a disposición de determinados tipos de operaciones de procesamiento

o futuras comunicaciones, la configuración estándar de esa aplicación debe ser siempre la más segura. Estos ajustes sólo se modifican si el usuario realiza un procedimiento de forma activa (por ejemplo, marcando una casilla o haciendo clic en un botón para indicar su consentimiento).

Como puedes ver, se puede garantizar la máxima privacidad de los datos utilizando todo tipo de medidas, que el RGPD anima a todos a aplicar en todo momento y en su mayor extensión. La privacidad de los datos no es un tema a olvidar o del que se pueda prescindir en un proyecto actual. Todo lo contrario. Es una cuestión que debe preocuparnos.

El futuro mostrará cómo las grandes y pequeñas empresas, los sujetos individuales de los datos (que pueden ser incitados a actuar por las organizaciones de consumidores o los sindicatos), las autoridades de supervisión y la propia UE se ocuparán del RGPD. No cabe duda de que los tribunales tendrán que ocuparse de algunos litigios complejos. Además, será difícil predecir cuáles serán las respuestas a las muchas preguntas que aún quedan por responder. Sin embargo, una cosa nos queda clara: la privacidad de los datos es algo que hay que tener en cuenta, y lo más probable es que siempre sea así.

Si tiene alguna pregunta o comentario, por favor escríbanos a
rgpd@mailteck-customercomms.com

Fuente: D'Huys, V. 22 January 2018.
www.groupjoos.com

www.mailteck.com - www.customercomms.com