Expansión

SUPLEMENTO ESPECIAL | SÁBADO, 26 DE MAYO DE 2018

www.expansion.com

Las 20 claves de la nueva Ley de Protección de Datos

LAS 20 CLAVES DE LA NUEVA LEY DE PROTECCIÓN DE DATOS

Todo lo que ha cambiado en la Protección de Datos

Mercedes Serraller

Desde ayer, viernes 25 de mayo, todas las empresas y organizaciones, públicas o privadas, tendrán que aplicar el nuevo Reglamento General de Protección de Datos (RGPD), ya que no existe ningún periodo transitorio o de gracia adicional. Esta norma europea, que unifica las diferentes leyes nacionales que había hasta el momento, mantiene parte de la normativa que estaba en vigor, pero contiene obligaciones que no existían hasta la fecha. También se aplicará una nueva Ley de Protección de Datos, cuya reforma está en tramitación, que especificará y complementará ciertas partes del RGPD, pero sin modificarlo. EXPANSIÓN le ofrece las 20 claves del Reglamento y del nuevo escenario, elaboración que ha contado con contenidos de Apuntes & Consejos de Indicator y de RSM Spain.

El primer paso para las empresas es identificar las áreas de riesgo y documentar e inventariar los tratamientos de datos personales que llevan a cabo. La Agencia Española de Protección de Datos (AEPD) ha publicado una lista de verificación y dispone de una herramienta que permite valorar la situación.

Gonzalo F. Gállego, socio de Propiedad Intelectual de Hogan Lovells, advierte, ante la llegada masiva de emails de consentimiento en los últimos días, de que "no todos los tratamientos requieren consentimiento", pero subraya que el nuevo Reglamento "sí establece cambios importantes", como la eliminación del consentimiento tácito (por silencio), la exigencia de la realización de una evaluación de impacto para ciertos tratamientos, o la obligatoriedad de comunicar en un plazo de 72 horas a la AEPD las violaciones de la seguridad de los datos personales.

1 Afectados

Todas las empresas y las organizaciones. No importa si el tratamiento de datos de carácter personal lo realiza un autónomo o una sociedad. El RGPD no realiza ninguna distinción en este sentido, por lo que quienes desarrollen una actividad empresarial, deberán cumplir con esta norma independientemente de cómo la realicen.

1.1. Datos personales

Los datos personales son toda información relativa a una persona física viva identificada o identificable (no las personas jurídicas), e incluyen, por ejemplo, el nombre, los apellidos, el domicilio, la dirección de correo electrónico o los datos de localización del mapa de su móvil. Éste suele ser el caso de los datos que las empresas puedan tener sobre sus empleados, clientes o proveedores.

1.2. Pymes

El Reglamento afecta a las pymes, aunque tengan muy pocos trabajadores y no contacten con consumidores finales. Si no tratan con consumidores finales, sí lo hacen con sus empleados, proveedores, etcétera con independencia de su tamaño o del volumen de datos que manejen.

1.3. Subcontratas

Las empresas que prestan servicios a terceros, subcontratas o *outsourcing*, también deben cumplir la norma. Deberán estar en condiciones de acreditar y garantizar ante sus clientes que se han adaptado y cumplen con esta norma.

1.4. Empresas de fuera de la UE

Las empresas con sede fuera de la Unión Europea (UE) que hagan venta online en algunos países de Europa tendrán que cumplir con la norma. Todas las compañías que ofrezcan bienes y servicios y manejen datos de ciudadanos de la UE deben someterse al nuevo Reglamento de Protección de Datos, aunque tengan su sede fuera.

1.5. Auditorías

Si una empresa tiene hecha una auditoría en protección de datos, ésta no es suficiente para adaptarse al nuevo Reglamento. "Es un buen punto de partida, pero debe tener en cuenta que el RGPD establece nuevas obligaciones. Por eso, tendrán

¿Y ahora qué?

Borja Carvajal Borrero

Director responsable de Regulatorio, Administrativo y Competencia de KPMG Abogados

Tras algunas semanas de bombardeo continuo sobre el asunto, por todos los flancos, a nadie le debería haber pasado inadvertido que ayer se produjo por fin la esperada entrada efectiva del Reglamento General de Protección de Datos (RGPD). Una vez expirados los dos años de moratoria desde su aprobación en 2016, en los que una gran parte de las mayores empresas de nuestro país han afrontado un proceso de adecuación prolongado y costoso, parece un buen momento para hacer balance del camino recorrido y del pendiente por hacer.

El RGPD fue aprobado el año 2016 para sustituir a una normativa europea previa, la Directiva de 1995, que por el avance de la tecnología y de la sociedad, resultaba evidente que había quedado obsoleta. La LOPD y su Reglamento de desarrollo en España, a pesar de ser de los más avanzados en su género, no han corrido mejor suerte durante sus casi veinte años de vigencia.

Sin duda, el gran cambio que implica el RGPD sobre la normativa previa se centra en la nueva cultura de cumplimiento en materia de privacidad que conlleva. Mientras que a finales de los 90 era posible definir desde la normativa las medidas de salvaguarda que eran exigibles a determinada categoría o fichero de datos, lo cierto es que en este momento no lo es. La Unión Europea, consciente de ello, ha optado por trasladar a las empresas la obligación de evaluar y gestionar proactivamente los riesgos en privacidad de su actividad. Y, lo que es más importante, de forma armónica y homogénea en todos los Estados miembros.

Este punto, el de la homogeneidad en la aplicación de la norma, es ciertamente uno de los aspectos en los que los distintos reguladores en la materia deberán trabajar intensamente durante los próximos años. La Agencia Española ha ido emitiendo durante estos últimos meses numerosos comunicados, guías, presentaciones e informes interpretativos sobre el RGPD. Gusten o no los distintos criterios que se han definido en los mismos, lo cierto es que ha sido un ejercicio de divulgación y concienciación ejemplar que no ha sido replicado por igual en todos los países de la Unión.

El hecho de que otros reguladores europeos no hayan exteriorizado su parecer sobre determinadas cuestiones que podrían resultar dudosas, ha conllevado numerosas incertidumbres en los procesos de adecuación de grupos con presencia en varios países de la UE. Y en el corto plazo, ello dificultará notablemente que se lleve a cabo una homogeneización de criterios sobre el Reglamento en todo el territorio de ésta. Es de esperar que esta situación se ataje pronto con la efectividad de los mecanismos de coherencia previstos en el propio RGPD (Co-

que revisarlas y adecuar sus políticas de privacidad", explica Life Abogados.

2

Multas

Infringir la normativa se sanciona con multas económicas que pueden ser muy elevadas. En este sentido, el RGPD clasifica las infracciones en dos categorías: menos graves y más graves. El régimen sancionador se aplica a los responsables y encargados del tratamiento. En cambio, no se aplica al delegado de protección de datos. Para fijar la cuantía de la sanción dentro de los márgenes establecidos para cada una de las infracciones, se tienen en cuenta una serie de criterios de graduación, como el volumen de negocio o actividad del infractor, el grado de intencionalidad, el que haya reincidencia o no, los perjuicios causados a las personas interesadas y a terceras personas, entre otros.

2.1. Menos graves

Las menos graves se sancionan con hasta 10 millones de euros o el 2% del volumen de facturación anual de la empresa (la más alta de las dos).

2.2. Más graves

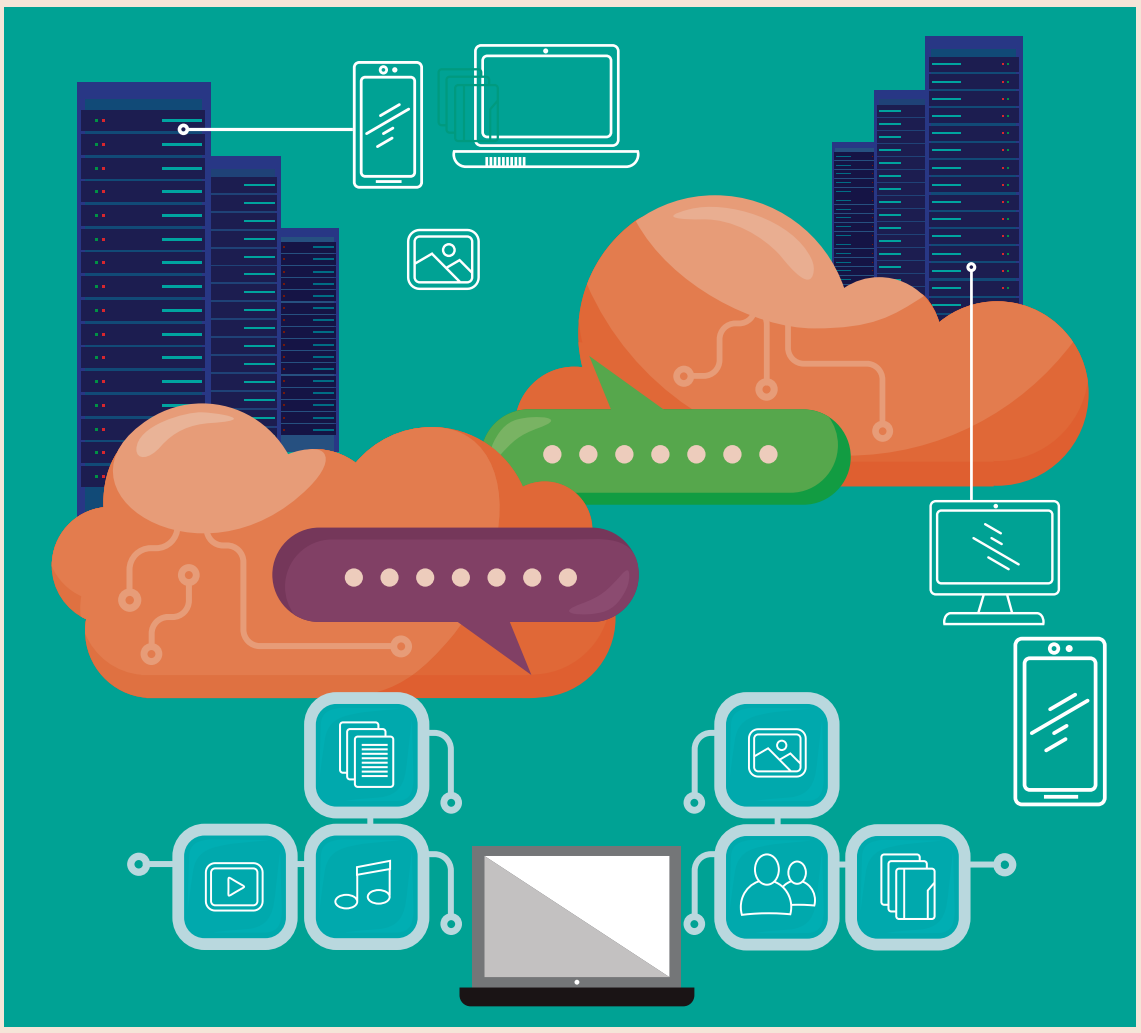
Las más graves se sancionan con multas que pueden alcanzar hasta 20 millones de euros o el 4% del volumen de facturación anual de la empresa (la más alta de las dos).

2.3. Apercibimiento

La sanción económica puede ser sustituida por un apercibimiento para que el infractor adopte las medidas correctoras que se le indiquen. Esta posibilidad es excepcional. La Agencia Española de Protección de Datos tiene potestad discrecional para aplicarla en función de la naturaleza de los hechos. Cuando la AEPD apercibe en lugar de imponer una sanción económica, el responsable del fichero o el encargado del tratamiento deberá acreditar la adopción de las medidas correctoras indicadas por la AEPD en su resolución de apercibimiento. En caso de no acreditarse el cumplimiento de estas medidas, la AEPD ordenará la apertura de un procedimiento sancionador por dicho incumplimiento, pudiendo imponer una sanción por infracción muy grave.

La AEPD ha aplicado el apercibimiento como alternativa a la sanción económica en numerosas ocasiones. Por ejemplo, por el hecho de instalar un sistema de videovigilancia en las zonas comunes de la empresa sin informar a los afectados. También por el hecho de informar a los clientes de la creación de la página web de la empresa enviándoles un correo electrónico sin copia oculta (de manera que todos los destinatarios podían ver las direcciones de los demás).

En cambio, se ha denegado el apercibimiento y se ha impuesto una multa en los casos de abandono de documentos en la vía pública; envío de comunicaciones comerciales por email o SMS sin el consentimiento previo y expreso de los destinatarios (salvo si éstos eran clientes de la empresa); envío de mensajes electrónicos a destinatarios múltiples sin copia oculta (se trataba de datos especialmente protegidos); difusión en una red social del parte de baja médica de una empleada; publicidad en Internet de datos médicos por parte de una clínica (aunque se trató de un error puntual), y difusión en Internet por parte de la empresa del currículo de un trabajador.



3

Delegado

Nombrar un delegado de protección de datos (DPD) o *data protection officer* es obligatorio para todas las autoridades y organismos públicos, así como para empresas que realicen una observación habitual y sistemática de las personas a gran escala o que tengan entre sus actividades principales el tratamiento de datos sensibles. También afecta a los centros docentes, operadores de telecomunicaciones, entidades financieras, compañías de publicidad y prospección comercial, centros sanitarios, operadores de juego y empresas de seguridad privada, entre otras.

Así, la nueva normativa europea establece, en su artículo 37, una serie de supuestos y actividades en los que será obligatorio contar con la figura del *data protection officer*: cuando el tratamiento de esta información se realice a través de un organismo o Administración Pública, a excepción de los tribunales; cuando la actividad principal de la empresa implique el tratamiento y observación habitual y regular de las políticas de protección de datos fijadas en el nuevo reglamento europeo, y cuando las actividades principales del encargado o la empresa consistan en el tratamiento a gran escala de datos personales (según los supuestos del artículo 9) y de aquellas informaciones y datos referidos a condenas y sanciones.

3.1. Certificación

La AEPD presentó en julio de 2017, junto a la Entidad Nacional de Acreditación (ENAC), el primer esquema de certificación de DPD y, a principios de año, emitió la primera autorización a ANF AC, que podrá certificar la idoneidad de todos los expertos que aspiren a ser delegados de protección de datos.

Para que las autoridades acreditadas puedan certificar que un trabajador es adecuado, éste deberá ser capaz de recabar información para determinar las actividades de tratamiento; analizar y comprobar la conformidad de las actividades de tratamiento e informar, asesorar y emitir recomendaciones al encargado del tratamiento.

También tendrá que asesorar en la aplicación del principio de la protección de datos por diseño y por defecto. Europeo de Protección de Datos, ventanilla única, procedimiento de resolución de conflictos, etcétera).

Una de las cuestiones que más se han discutido en los últimos meses es el alcance que cabe dar al interés legítimo como base legitimadora del tratamiento de datos con fines comerciales. Este asunto ha adquirido especial trascendencia con la puesta en funcionamiento del RGPD, puesto que éste implica invalidar una gran parte de los consentimientos que se venían utilizando en nuestro país para realizar campañas de marketing.

A pesar del impacto en el negocio que una interpretación restrictiva de este aspecto podría tener en numerosas compañías, se ha cuestionado la posibilidad de reconducir por esta vía enriquecimientos y perfilados de datos complejos, la promoción de productos de terceros o no vinculados con los ya contratados, así como las cesiones de datos entre empresas. Para salvaguardar el más elemental principio de seguridad jurídica, parece exigible que esta cuestión quede perfilada con mayor nitidez a nivel europeo a la mayor brevedad posible.

Otro de los aspectos en los que queda trabajo por realizar es el relativo al alcance y forma del derecho a la portabilidad de los datos. En la práctica, el impacto que una interpretación amplia de este derecho podría conllevar desde la perspectiva de la competencia entre empresas rivales, ha supuesto un lógico recelo a configurarlos de forma generosa en los proyectos de adecuación. Un freno más en este frente, sin duda, se refiere a los necesarios desarrollos informáticos que se requieren para automatizar los procesos ante un posible escenario de ejercicio generalizado del derecho. Por la relevancia de la materia, parece lógico pensar que la práctica administrativa del RGPD nos dará pronto pistas sobre cómo habrá de aplicarse este nuevo derecho en los distintos sectores, incluso según avance la tramitación de los distintos Códigos de Conducta que se encuentran en preparación.

La adecuación de los contratos entre responsables y encargados del tratamiento parecía, a priori, uno de los puntos que más carga de trabajo podría haber generado en los proyectos de adecuación al RGPD de grandes empresas. El régimen transitorio previsto en el Proyecto de Ley de LOPD sobre esta materia (y la expectativa razonable de que sea aplicado, al menos desde una perspectiva sancionadora, aun cuando no haya sido aprobado todavía) ha venido a relajar la urgencia de afrontar este complejo proceso. Con todo, se trata de un melón que más pronto que tarde habrá que abrir.

La manifestación más relevante de la novedosa cultura de cumplimiento en privacidad que conlleva el RGPD se encuentra en la exigencia de la nueva figura del delegado de protección de datos. La identificación y contratación, en su caso, de los perfiles idóneos para cubrir la plaza y dotarles de los medios necesarios han sido, también, otros de los grandes retos que han tenido que afrontar las empresas estos últimos meses.

En gran medida, el acierto en esta decisión condicionará la suerte de las entidades en su mayor o menor adecuación al RGPD. Hasta ahora nos hemos limitado a limpiar la casa, pero lo realmente importante es que ésta se encuentre limpia en todo momento. O dicho de otra forma, el foco debería ponerse ahora en pasar del modo "proyecto de adecuación" al *business as usual*.

to; aconsejar si se debe llevar a cabo o no una evaluación de impacto de protección de datos, y qué metodología debe seguirse al efectuar este tipo de valoración. Por otro lado, deberá ser capaz de recabar información para supervisar el registro de las operaciones de tratamiento; así como priorizar sus actividades y centrar sus esfuerzos en las cuestiones que presenten mayores riesgos.

3.2. Requisitos

Además de todas estas capacidades, según explica la AEPD, deberán cumplir alguno de los siguientes requisitos: justificar una experiencia profesional de, al menos, cinco años en proyectos o actividades relacionadas con las funciones del DPD en materia de protección de datos. Tener una experiencia demostrable de, al menos, tres años en proyectos o actividades y tareas relacionadas con las funciones del DPD en materia de protección de datos, y una formación mínima reconocida de 60 horas en relación con las materias incluidas en el programa del esquema; acreditar una experiencia profesional de, al menos, dos años en proyectos o actividades y tareas relacionadas con las funciones del DPD, y una formación mínima reconocida de 100 horas en relación con las materias incluidas en el programa; o, por último, justificar una formación mínima reconocida de 180 horas en relación con las materias del programa del texto elaborado por la AEPD.

El DPD puede ser alguien interno de la empresa o externo (como un asesor a quien se encargue esta función mediante un contrato de servicios). En todo caso, el DPD no puede ser cualquier persona, ya que es necesario que tenga conocimientos jurídicos y prácticos en materia de protección de datos y no se encuentre en una situación de conflicto de interés.

3.3. Responsable y encargado

No se debe confundir al DPD con otras figuras. El responsable del tratamiento es quien decide sobre el contenido, uso y finalidad de los tratamientos de datos. El encargado trata datos de carácter personal por cuenta del responsable.

4

Autoridades de supervisión

Aunque estos cambios normativos derivan de una normativa de ámbito europeo, el organismo encargado de velar por el cumplimiento del RGPD y de la nueva LOPD seguirá siendo la Agencia Española de Protección de Datos. En este sentido, la AEPD ha creado una sección específica en su página web donde publica todo tipo de información de interés sobre el RGPD. Puede acceder a ella a través del siguiente enlace: *http://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php*.

5

Seguridad

La normativa vigente hasta ahora establecía con detalle y de forma exhaustiva las medidas de seguridad que debían aplicarse según el tipo de datos objeto de tratamiento. En cambio, con el nuevo RGPD, tanto el responsable como el encargado del tratamiento siguen estando obligados a adoptar medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos, según los riesgos que se hayan detectado al realizar el análisis previo. Sin embargo, el nuevo RGPD no especifica qué medidas de seguridad concretas hay que aplicar en cada caso, sino que éstas se deben determinar por el responsable o por el encargado según diversas variables: el estado de la técnica, los riesgos que existan para los derechos y libertades de los interesados, la naturaleza, el alcance, el contexto y los fines del tratamiento y los costes de aplicar las medidas. No obstante, la propia AEPD ha señalado que, en algunos casos, se pueden seguir aplicando las mismas medidas de seguridad que establece la normativa hasta ahora vigente si del análisis de riesgos se concluye que dichas medidas son idóneas para ofrecer un nivel de seguridad adecuado (en caso contrario, será necesario completar dichas medidas o prescindir de alguna de ellas).

5.1. Niveles de seguridad

En muchos casos se pueden seguir aplicando las mismas medidas de seguridad que establecía el Reglamento de Desarrollo de la LOPD si éstas ya ofrecen un nivel adecuado de seguridad. Por tanto, cabe recordar que dicha norma establece tres niveles de seguridad (básico, medio y alto), dependiendo de la naturaleza de los datos personales tratados. Estos niveles de seguridad son acumulativos. Por tanto, los ficheros o tratamientos de datos de carácter personal de nivel básico sólo deben adoptar las medidas de seguridad de nivel básico. Los ficheros y tratamientos de datos de nivel medio deben adoptar tanto las medidas de seguridad de nivel básico como las de nivel medio.

El papel del auditor interno

Pablo González Melgar

Experto en RGPD
Instituto de Auditores Internos de España

Desde el 25 de mayo, el Reglamento General de Protección de Datos (RGPD) es de obligado cumplimiento para las empresas establecidas en algún Estado miembro de la Unión Europea, independientemente de que el tratamiento de los datos personales tenga lugar o no en la propia UE. También aplica a organizaciones no establecidas en la Unión, pero que traten datos personales de interesados que residan en ella.

Esta norma pretende homogeneizar entre los países miembros los principios y garantías con respecto a los derechos y libertades de las personas físicas en lo relativo al tratamiento de datos de carácter personal.

Para poder cumplir con estos principios fundamentales, las organizaciones (públicas o privadas) requieren, indefectiblemente, alcanzar la definición e implantación de un Modelo de Gobierno de la Privacidad que regule las actividades que conforman los procesos de tratamiento de datos personales (recogida, almacenamiento, consulta, comunicación, difusión, supresión, etcétera).

Desde el punto de vista estratégico, este modelo debe quedar sustentado por una Política de Privacidad y Protección de Datos aprobada por la Dirección de la organización, que marque directrices de actuación para el tratamiento de los datos y se alinee con las piedras angulares que conforman la norma RGPD: los Principios de Responsabilidad Proactiva (*Accountability*), Privacidad en el Diseño (*Privacy by design*) y Privacidad por Defecto (*Privacy by Default*).

Desde el punto de vista operativo, el modelo debe tener un enfoque de análisis, evaluación y tratamiento de los riesgos, de forma que las medidas técnicas y organizativas necesarias para ello respondan a una estrategia bien definida e implantada para mitigar los riesgos en materia de protección de datos.

En definitiva, esta nueva normativa no detalla las actividades de adecuación concretas para cumplir con la norma, sino solo los principios fundamentales que deben regir la definición e implantación del modelo de Gobierno de la Privacidad que deben formalizar las organizaciones para garantizar la privacidad de los datos personales.

Los ficheros y tratamientos de datos de nivel alto deben aplicar las medidas previstas en los niveles básico, medio y alto.

5.2. Nivel alto

Son ficheros o tratamientos de nivel alto, entre otros, los que se refieren a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. Una de las medidas de seguridad que se debe implantar en estos ficheros de nivel alto (si son automatizados) es, por ejemplo, la del registro de accesos, de manera que quede registrado el usuario que ha intentado acceder al fichero, la hora, el fichero, el tipo de acceso y si dicho acceso ha sido autorizado o denegado.

5.3. Nivel medio

Son ficheros o tratamientos de nivel medio, entre otros, aquellos relativos a la prestación de servicios de solvencia patrimonial y créditos, aquellos de los que sean responsables entidades financieras para las finalidades relacionadas con la prestación de servicios financieros y aquellos que contengan un conjunto de datos que ofrezcan una definición de las características o de la personalidad y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de las personas. Una de las medidas que se debe implantar para estos ficheros o tratamientos de datos de nivel medio es la realización de una auditoría (interna o externa) cada dos años a fin de verificar que se cumplen las medidas de seguridad que exige la normativa de protección de datos.

5.4. Nivel básico

Es un fichero o tratamiento de datos básico cualquier otro fichero distinto a los indicados que contenga datos de carácter personal. Una de las medidas de seguridad de nivel básico (y que, por tanto, debe implantarse en todo tipo de ficheros automatizados) es que se establezca un procedimiento de asignación y distribución de contraseñas y que las contraseñas se cambien, al menos, una vez al año. También se consideran de nivel básico los ficheros o tratamientos que contienen datos de nivel medio o alto sólo de forma accidental o accesoria, pero sin guardar relación con su finalidad. Por ejemplo, un hotel dispone de los datos de alergias alimentarias de un cliente. Éste es un dato de nivel alto por referirse a la salud, pero está en el fichero de forma incidental, pues la finalidad de dicho fichero es el hospedaje.

5.5. El documento de seguridad

Aunque el nuevo RGPD no exige expresamente que se confeccione un *documento de seguridad*, es aconsejable que se haga, en los mismos términos que exigía la normativa anterior. En este sentido, el documento de seguridad es un documento interno que debe mantenerse actualizado en todo momento y exhibirse en caso de inspección por parte de la AEPD. También debe demostrarse que se está aplicando de forma efectiva. Las menciones mínimas del documento de seguridad son las siguientes: ámbito de aplicación, especificando de forma detallada los recursos protegidos (servidores, ordenadores, tabletas, discos duros externos u otros elementos de almacenaje con datos de carácter personal); medidas, normas, procedimientos de actuación, reglas y estándares para garantizar el nivel de seguridad exigido; funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal; estructura de los ficheros y descripción de los sistemas de información que los tratan; procedimiento de notificación, gestión y respuesta ante incidencias; procedimientos de realización de copias de respaldo y de recuperación de datos en los ficheros o tratamientos automatizados. Respecto a las medidas adoptadas para el transporte, la destrucción y/o la reutilización de soportes y documentos, cuando se trate de ficheros o tratamientos de datos de nivel medio o alto, en el documento de seguridad se debe incluir, además de los apartados anteriores, la identificación del responsable de seguridad y la obligación de realizar una auditoría bianual para verificar la correcta cumplimentación de las medidas de seguridad.

6
Análisis de riesgos

Un programa estándar ya no sirve para asegurarse el cumplimiento. En el caso del tratamiento de informaciones especialmente sensibles es necesario llevar a cabo un análisis de riesgos, así como una evaluación del impacto. La AEPD ha publicado una lista de verificación que permitirá valorar la situación de la empresa. Se estructura como un listado de preguntas que cada organización deberá hacerse y responder adecuadamente para así determinar cuál es su grado de cumplimiento.

6.1. La herramienta de la AEPD

La AEPD dispone de una herramienta que a través de preguntas muy concretas permite valorar su situación respecto del tratamiento de datos personales que lleva a cabo. En caso de confirmar que se encuentra en un nivel bajo de riesgo, la herramienta genera diversos documentos adaptados a su empresa para que cumpla las obligaciones que establece el RGPD (cláusulas informativas, contractuales...). *https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/herramientas_ayuda/index-ides-idphp.php*.

El uso de la herramienta es anónimo, y la AEPD no identifica a quienes la usan. Ni el uso de esta herramienta ni la obtención de los documentos resultantes implican el cumplimiento automático del RGPD (de hecho, estas herramientas no resultan útiles para empresas que tratan datos de riesgo).

Esta herramienta toma en cuenta hasta tres factores de riesgo. En primer lugar, si la empresa pertenece a sanidad, solvencia patrimonial y crédito, generación y uso de perfiles, actividades políticas, sindicales y religiosas, servicios de telecomunicaciones, seguros, entidades bancarias y financieras, actividades de servicios sociales, publicidad y videovigilancia masiva. Un segundo factor es tratar datos que revelen origen étnico o racial; datos de opiniones políticas o religión; datos de afiliación sindical (excepto cuotas sindicales); datos genéticos; datos biométricos dirigidos a identificar de manera unívoca a una persona; datos de salud física o mental; datos relativos a la vida sexual o a la orientación sexual; datos relativos a condenas o infracciones penales, y geolocalización. En tercer lugar, se sitúa el factor de riesgo de que la empresa haga o analice perfiles; publicidad y prospección comercial masiva a potenciales clientes; prestación de servicios de explotación de redes públicas o servicios de comunicaciones electrónicas; gestionar los asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas, fundaciones y otras entidades sin ánimo de lucro cuya finalidad sea política, filosófica, religiosa o sindical; gestión, control sanitario o venta de medicamentos e historial clínico o sanitario.

7
Brechas de seguridad

Antes de la entrada en vigor del RGPD, la obligación de notificar las brechas de seguridad o violaciones de seguridad se limitaba a los operadores de servicios de comunicaciones electrónicas disponibles al público. Ahora se entenderá que existe una brecha de seguridad en aquellos casos en los que la violación de la seguridad de los datos (*data breach*), como los presenciados últimamente en casos tales como el de Facebook y Cambridge Analytica.

El principio de Privacidad en el Diseño demanda proactividad desde el instante preciso que se plantea la concepción o diseño de una nueva iniciativa de tratamiento de datos, evitando cualquier incumplimiento de los principios de la norma cuando dicha iniciativa pase a ser un proceso de tratamiento de datos, esto es, la explotación de los datos personales en un entorno real. Para entonces, cualquier "error" en el proceso de tratamiento de datos, ya será una vulneración de los derechos y libertades de las personas físicas en materia de protección de datos y, por tanto, será de poca utilidad la consideración de acciones correctivas. El éxito de cumplimiento del RGPD se focaliza en prevenir eventos no deseados, y no tanto en la corrección de incidentes acaecidos.

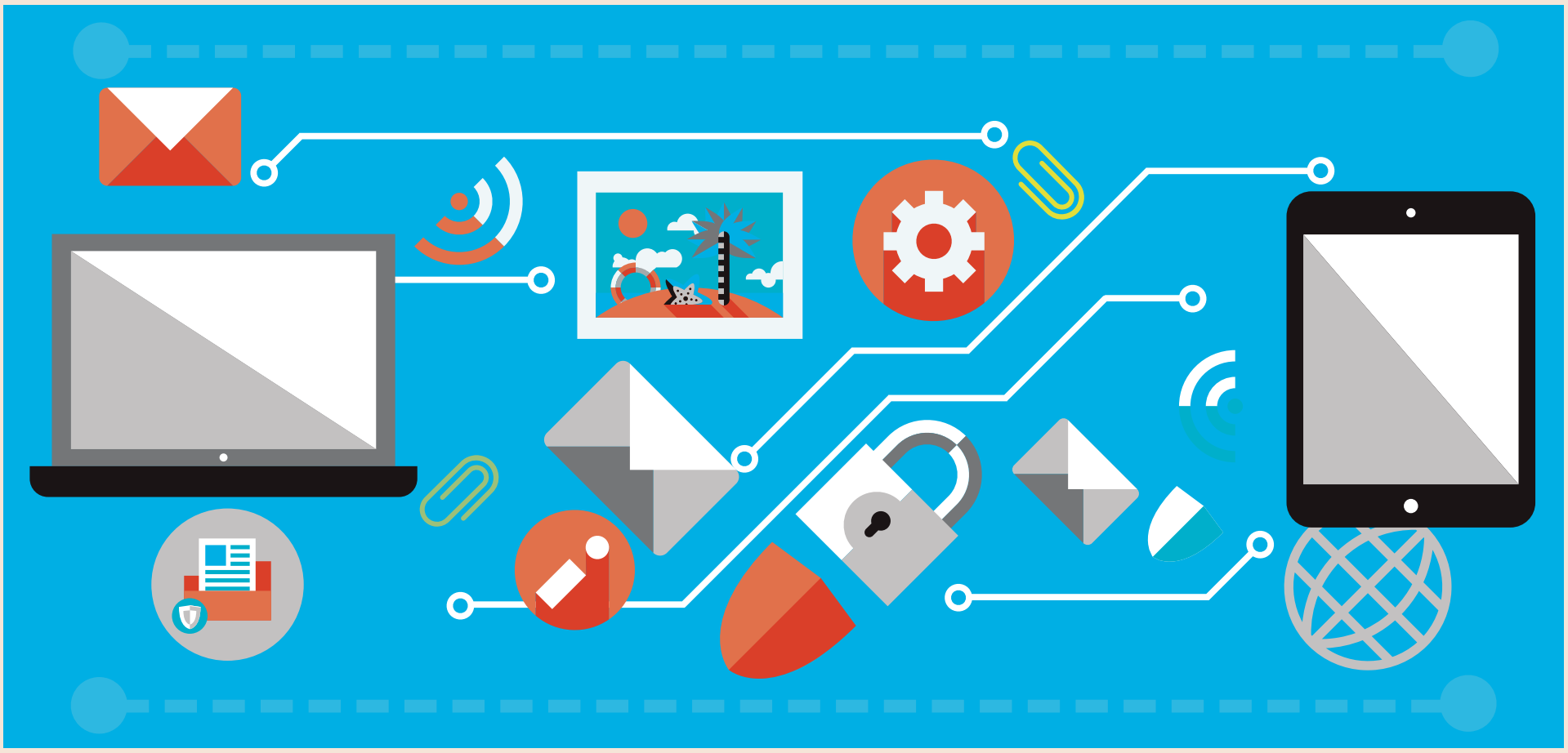
Esta indefinición de la norma es vista como una debilidad por aquellos que pretenden acometer la adecuación como si fuese un proyecto (caracterizado por la identificación de fechas de inicio y fin de actividades), en lugar de implantar un programa de gobierno de la privacidad que a partir del 25 de mayo se mantenga en vigor expuesto a mantenimiento y mejora continua sin fecha de caducidad (con un enfoque basado en un sistema de gestión de la privacidad).

El dinamismo que presenta el tratamiento de los datos en las organizaciones no permite un enfoque de proyecto de adecuación. Solo mediante la formalización del modelo de Gobierno, la definición de una estructura organizativa con el detalle de funciones y responsabilidades, y la adopción de una actitud preventiva frente a los riesgos de confidencialidad, disponibilidad e integridad para los datos personales, se podrán evitar escenarios de violación de

El papel del auditor interno con respecto a la adaptación es fundamental

El papel del auditor interno con respecto a la adaptación al Reglamento es fundamental, ya que podrá revisar el entorno de controles habilitados en el contexto del modelo de Gobierno de la Privacidad con el objeto de obtener garantías razonables de que los principios fundamentales recogidos en la norma están siendo atendidos.

Su interrelación con la función de monitorización identificada en dicho Modelo de Gobierno de la Privacidad, focalizada en el trabajo del delegado de Protección de Datos, es prioritaria ya que, solo de esta forma, se podrá alcanzar un modelo de aseguramiento en lo relativo al cumplimiento de los principios, derechos y obligaciones recogidas en la norma RGPD.



guridad ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Los responsables de tratamiento de datos de carácter personal estarán obligados a notificar a la autoridad de control de aquellas brechas de seguridad que constituyan un riesgo para los derechos y las libertades de las personas físicas. En aquellos casos en los que la empresa determine que la brecha de seguridad constituya un riesgo para los derechos y libertades de las personas físicas, deberá, en todo caso, proceder a su notificación a la autoridad de control sin dilación indebida y, a más tardar, 72 horas después de que haya tenido constancia de ella. Si dicha notificación no es posible en el plazo de 72 horas, deberá acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida. Como mínimo, esta notificación deberá contener una descripción de la naturaleza de la violación de seguridad (incluyendo, cuando sea posible, las categorías y número aproximado de afectados y de registros de datos personales afectados), así como los detalles de contacto del DPD de la empresa, las posibles consecuencias de la brecha de seguridad y las medidas de seguridad adoptadas o propuestas por el responsable del tratamiento.

8

Información y consentimiento

Si la empresa obtiene datos personales (de clientes, trabajadores, usuarios de su página web, etc.), está obligada a informar al interesado de los tratamientos o usos que va a realizar con esos datos. La obligación de informar corresponde a su empresa si actúa como responsable del tratamiento. Este derecho de información de los interesados es esencial, ya que pretende que el afectado pueda prestar su consentimiento (específico, informado e inequívoco) para que se traten sus datos personales, y que pueda ejercer los derechos de acceso, rectificación, limitación al tratamiento, supresión, portabilidad y oposición que la normativa reconoce a los interesados. Básicamente, usted debe informar a los interesados (a continuación, le indicamos cuándo debe hacerlo).

8.1. Cuándo obtener la información

Si la empresa obtiene los datos directamente del propio interesado, debe proporcionarle la información indicada en el momento en el que solicite sus datos, previamente a su recogida o registro. En cambio, si obtiene los datos de personas distintas al interesado (por ejemplo, por una cesión legítima de datos), debe informar al interesado de esa recogida de datos en un plazo razonable, pero, en cualquier caso, antes de un mes desde que se obtuvieron los datos personales o, en su defecto, en la primera comunicación con el interesado.

8.2. Cómo obtener el consentimiento informado

Para que se pueda tratar lícitamente los datos personales de sus clientes (o de cualquier otra categoría de interesados), es necesario que, además de informarles en los términos indicados, solicite y obtenga su consentimiento previo e inequívoco. Así, se elimina el consentimiento tácito (por silencio), lo que obligará a las empresas a recabar un nuevo consentimiento para poder mantener todos aquellos datos que en el pasado se obtuvieron tácitamente o buscarles otra cobertura legal. A estos efectos, se entiende que existe dicho consentimiento inequívoco cuando éste se ha prestado mediante una declaración o una clara acción afirmativa del interesado. A diferencia de la normativa anterior, con el RGPD ya no se admiten formas de consentimiento tácito o por omisión, ya que éstas se basan en la inacción del interesado. Puede suceder que su empresa esté tratando unos datos personales desde antes de la aplicación del RGPD, y que lo haga sobre la base del consentimiento del afectado. Pues bien, en este caso dicho consentimiento sigue siendo válido, pero sólo si se prestó de la forma en que exige el RGPD, es decir, sólo si se prestó mediante una declaración o acción afirmativa del afectado.

8.3. Revocación

El afectado tiene derecho a revocar su consentimiento en cualquier mo-

Fronteras en el consentimiento

Isabel Moreno Martínez-Ortiz

Responsable de Asesoría Jurídica en EUDE Business School

A partir del 25 de mayo, entra en vigor el Reglamento de la Unión Europea 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta a tratamiento de datos personales y a la libre circulación de dicha información (GDPR, por sus siglas en inglés). Se abre, así, un panorama que ofrece un marco más sólido y coherente que evite la aplicación fragmentada, la inseguridad jurídica y las diferencias en la protección de los derechos y libertades en los Estados miembro de la Unión Europea. Lo fundamental para las compañías es desarrollar un plan de cumplimiento donde identifiquen las amenazas y riesgos a los que está expuesta una actividad de tratamiento de datos personales; estableciendo una descripción detallada del contexto de la actividad empresarial y los elementos más relevantes que intervienen en la misma para poder gestionar los riesgos con el fin de minimizarlos al máximo.

La empresa que detecte cualquier filtración o hackeo deberá notificarlo a los interesados y a las autoridades de control. Nombrar un delegado de protección de datos es una obligación y constituye uno de los elementos clave del GDPR y un garante del cumplimiento de la normativa de protección de datos de la empresa.

También se implanta la creación de mecanismos de certificación y sellos de protección de datos que serán expedidos por las autoridades de control. Es una novedad la introducción de los conceptos de privacidad por el diseño y por defecto y la obligación de llevar a cabo evaluaciones de impacto en materia de protección de datos.

Si el usuario considera que se han vulnerado sus derechos, podrá formular una reclamación, sin necesidad de contar con un abogado o procurador y sin coste alguno. La nueva normativa incluye la creación de una ventanilla única como sistema que permita a cualquier ciudadano europeo presentar una reclamación en su propio país, aunque la empresa denunciada tenga sede en otro Estado miembro.

Los pilares sobre los que se asienta el nuevo modelo de protección de datos son la licitud, lealtad y transparencia con la que deben tratarse la

mento y a través de un medio sencillo y gratuito. La retirada del consentimiento no afecta al tratamiento de los datos que se haya realizado anteriormente, pues éste se basó en el consentimiento prestado antes de su retirada.

9

Cesión de datos a terceros

No toda comunicación o revelación de datos a un tercero implica una cesión de datos a efectos legales. En este sentido, cabe distinguir dos supuestos: la cesión de datos propiamente dicha y el acceso a datos para la prestación de un servicio. Habrá una cesión de datos si el tercero que los recibe puede aplicarlos a sus propias finalidades, decidiendo sobre el objeto y finalidad del tratamiento. En cambio, si quien recibe los datos se limita a efectuar determinadas operaciones sobre ellos, pero no decide sobre su finalidad, existirá un acceso a datos para la prestación de un servicio.

9.1. Requisitos

Para ceder datos de forma lícita, la empresa deberá contar con el consentimiento previo, específico e inequívoco de los titulares de dichos datos; que la cesión sea necesaria para la ejecución o desarrollo de una relación contractual; que constituya una obligación legal para el cedente; que obedezca a intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos, y que sirva para salvaguardar el interés vital del interesado o de otras personas.

La realización de una prestación de servicios con acceso a datos requiere la existencia de un contrato escrito que establezca expresamente las obligaciones del encargado del tratamiento. Con el RGPD, la responsabilidad última sobre el tratamiento sigue estando atribuida al responsable, que es quien determina la existencia del tratamiento y su finalidad. Ahora bien, el RGPD introduce cambios importantes en las relaciones responsable-encargado que su empresa deberá tomar en consideración independientemente de la posición que ocupe en el tratamiento de los datos.

Si la empresa es la responsable, tendrá que elegir únicamente encargados que ofrezcan garantías suficientes de que aplicarán medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con el RGPD. Este requisito también se aplica a los encargados cuando subcontraten operaciones de tratamiento con otros subencargados. Es aconsejable que exija una declaración por escrito de dicho encargado conforme cumplirá las exigencias del RGPD y que le solicite, además, una prueba del cumplimiento del RGPD antes de firmar el contrato y durante su vigencia.

Si, en cambio, la empresa es el encargado del tratamiento, hay que considerar la necesidad o conveniencia de mantener un registro de las actividades del tratamiento. La empresa tendrá que determinar las medidas de seguridad aplicables a los tratamientos que realice. Deberá designar un delegado de protección de datos en los casos previstos por el RGPD. Si destina los datos a una finalidad distinta a la establecida en el contrato suscrito con el responsable (o si los comunica o utiliza incumpliendo las estipulaciones de dicho contrato), responderá de las infracciones, pues se le considerará un responsable del tratamiento a estos efectos. Respecto a los contratos entre responsable y encargado firmados con anterioridad al 25 de mayo, el proyecto de nueva Ley de Protección de Datos prevé que sigan vigentes hasta su vencimiento, y si son de duración indefinida, hasta mayo de 2022.

10

Identificación y documentación

En materia de protección de datos personales, un fichero es todo conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso. Con el nuevo Reglamento ya no deberá notificarse la creación de estos ficheros de datos personales para su inscripción en el Registro General de Protección de Datos de la AEPD, como sí era obligatorio hasta ahora.

El tratamiento de datos personales es cualquier operación o conjunto de operaciones que se realicen sobre datos personales, ya sea por procedimientos automatizados o no. Con la nueva normativa, debe identificar los tratamientos de datos personales que realice para mantener un registro de actividades del tratamiento (si estuviera obligado).

11

Datos en la nube

Si se almacenan en los servidores del proveedor de *cloud* datos personales de terceros, deben tomarse precauciones, pues no todos los proveedores cumplen con los requisitos. Si el servidor en el que se almacenarán los datos está ubicado en España, hay que asegurare de que en el contrato el proveedor se compromete a no aplicar o utilizar los datos con fines distintos y que implantará medidas adecuadas al nivel de riesgo del tratamiento de datos, evitando que se destruyan, alteren o se acceda sin autorización. Si el servidor se localiza fuera de España pero dentro del Espacio Económico Europeo-EEE (UE e Islandia, Liechtenstein y Noruega), se debe verificar que se menciona el cumplimiento de las leyes del país en cuestión. Dado que la normativa europea está armonizada, no habrá necesidad de requerir garantías adicionales. En caso de ubicación fuera del EEE, por ejemplo en EEUU, asegúrese de que su proveedor está suscrito a los principios de "escudo de privacidad" (*privacy shield*). La UE reconoce este sistema como seguro.

12

Videovigilancia

Las cámaras no podrán obtener imágenes de espacios públicos, salvo que ello sea inevitable. Así, una cámara situada en la puerta principal o de entrada o salida de personas no deberá tomar imágenes de toda la calle en la que se encuentre. La colocación de cámaras debe respetar el principio de información personal. La limitación de la finalidad para la que se recoge es otra de las novedades que incorpora el GDPR, así como solicitar únicamente aquellos datos estrictamente necesarios. Se establece una limitación del plazo de conservación que no será superior al tiempo necesario para los fines del tratamiento. Para garantizar una seguridad adecuada de los datos, es imprescindible la formación e información que se facilita al personal involucrado en el tratamiento de los mismos.

Las sanciones económicas establecidas según lo dispuesto en el nuevo régimen sancionador del GDPR, suponen un aumento de las multas estipuladas hasta el momento. Tal es la importancia de adoptar las medidas necesarias para garantizar la seguridad de los datos de los usuarios, que las realizaciones del tratamiento sin las garantías necesarias podrían ascender a los 10 millones de euros o un 2% del volumen de negocio total anual del ejercicio financiero anterior, mientras que en la actualidad está penado con 300.000 euros.

Pero esto no es todo. La recogida de información sin especificar detalladamente las finalidades del tratamiento, la no supresión de los datos una vez hayan dejado de ser útiles para el objetivo con el que fueron recabados o finalizada la fase de bloqueo cuando existieran responsabilidades legales exigibles en vigor podrían suponer sanciones superiores a los 20 millones de euros o el 4% del volumen de negocio total anual del ejercicio financiero anterior. La misma multa se especifica para el tratamiento de los datos sin contar con el consentimiento explícito del interesado en los que el mismo fuera necesario o la realización de transferencias internacionales con destino a países que no garanticen un nivel adecuado de protección sin contar con la legitimación necesaria.

El auge de las tecnologías y, en especial, el uso de las redes sociales ha propiciado una falta de consciencia. Y es que no nos damos cuenta de la facilidad con la que nuestros datos personales trascienden a cualquier parte del mundo, dando acceso ilimitado al uso y disfrute de los mismos. Es necesario que cada uno establezca fronteras en el consentimiento que damos sobre nuestros datos y establezcamos las barreras necesarias para que no accedan aquellos que no deberían hacerlo. Sobre todo, es vital que eduquemos de esta forma a los menores y no nos expongamos con tanta facilidad, ni nosotros ni a los niños. Somos los únicos perjudicados debido a las graves consecuencias que puede llegar a tener la utilización fraudulenta de los datos personales. Ante esta realidad, es necesario que cada uno reflexionemos sobre nuestra propia conducta ante las nuevas tecnologías y nos hagamos responsables de nuestros actos, consentimientos y autorizaciones.

pio de proporcionalidad y el derecho a la intimidad. Por tanto, no deben colocarse de forma que capten imágenes en zonas privadas (como en los vestuarios de sus trabajadores), sólo en aquellas zonas donde razonablemente puedan cumplir con su finalidad. Asimismo, es necesario que se informe de la colocación de las cámaras con un cartel explicativo situado en un lugar visible de las zonas videovigiladas, en el que se informe, como mínimo, de la identidad de su empresa y la posibilidad de ejercitar los derechos que el RGPD reconoce a los interesados. Si las cámaras van a estar conectadas a una central de alarmas, será necesario que este servicio lo preste una empresa de seguridad privada. Si el sistema de videovigilancia instalado en la empresa graba las imágenes, deberá conservarse la grabación durante un plazo máximo de un mes, aunque podrán conservarse más tiempo si fuera necesario para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

13

Derechos del ciudadano

El RGPD contiene los tradicionales derechos de acceso, rectificación, cancelación y oposición, conocidos de forma conjunta bajo el acrónimo ARCO, a los que se suman los de limitación del tratamiento, portabilidad de datos o al olvido. La empresa, como responsable del tratamiento, debe facilitar a los interesados el ejercicio de sus derechos, y los procedimientos y las formas para ejercerlos deben ser visibles, accesibles y sencillos. Se exige, además, que sea posible la presentación de solicitudes por medios electrónicos.

14

'Spam'

Las empresas no pueden enviar correos electrónicos de forma indiscriminada, ya que lo prohíbe la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico. Deben evitar que sus envíos puedan ser calificados como *spam* (correo electrónico no deseado). Los destinatarios de la publicidad deben haber consentido previamente el envío. Por tanto, asegúrese de que en todos los formularios de su empresa donde se recogen datos de posibles clientes se menciona que éstos le autorizan expresamente a enviarles publicidad. No obstante, si el destinatario de la publicidad ya es cliente de su empresa y usted le envía información sobre productos o servicios similares de su

propia empresa a los que él le adquirió anteriormente, no será necesario disponer de esta autorización previa para poder enviarle publicidad. No olvide que el propio email debe informar al destinatario de la posibilidad de revocar el consentimiento otorgado inicialmente para el envío de la publicidad, e incluir una dirección electrónica a la que dirigirse para solicitar dicha revocación.

15

Divulgación de vídeos y fotos

La protección de los datos personales va mucho más allá de proteger una dirección de email o un número de teléfono. El contenido, por ejemplo, de un móvil también se considera información personal. Por eso, la legislación penaliza el acceso a estos dispositivos sin permiso, con el agravante de quienes además publican fotos o vídeos sin la autorización del interesado. En esta misma categoría se incluye la divulgación de datos disponibles de forma restringida, como puedan ser, por ejemplo, el historial médico de una persona.

16

Empleados

Los empleados tienen los mismos derechos que cualquier otro interesado, pero vienen condicionados por las características de propias de la relación laboral. Cuando se tratan datos personales cuyo uso está justificado, por ser necesarios para el mantenimiento de la relación laboral (ej. nombre y edad), no es necesario recabar el consentimiento de los trabajadores. Por el contrario, aquellos datos que pueden considerarse no necesarios para la prestación de servicios (ej. cuenta de correo electrónico personal) requerirán recabar el consentimiento de los trabajadores. En todo caso, los trabajadores deberían recibir información específica sobre el tipo de datos personales que están siendo tratados por la empresa, así como la finalidad de su tratamiento y la base legal para el mismo, así como las transferencias de datos a terceros que puedan producirse, según concretan desde Jausas. Se tiene que proporcionar información sobre los derechos que asisten a los trabajadores, junto con los datos de contacto de la empresa y de quienes hayan sido designados para responder las cuestiones planteadas por los trabajadores (si la empresa tuviera un delegado de Protección de Datos, se pondrían sus datos).

16.1. Cuando recogen datos

Cuando es el propio empleado de una compañía el que recoge datos de carácter personal, no es suficiente con exhibir el documento para lograr el consentimiento. Es el caso, por ejemplo, del recepcionista de un hotel. Además de solicitar al cliente que marque la casilla de autorización para tratar los datos personales, este empleado debe avisar de algunos aspectos básicos, como cuál es la finalidad de recopilar esa información. Además, si el empleado percibe cualquier tipo de brecha de seguridad, debe alertar a su superior inmediato. Hay departamentos que se consideran de riesgo por la información que manejan, como el área de márketing y comercial, en el que habrá que revisar todos los procesos, incluido cómo se fija el bonus (que no impliquen, por ejemplo, compartir datos personales).

17

Clientes

Como en el caso del resto de usuarios, será necesario que las empresas detallen explícitamente y con un lenguaje comprensible los datos e información personal requerida a sus clientes y sólo se podrá tratar los datos en caso que tengan un interés legítimo. El deber de informar a los afectados sobre el uso y las finalidades del tratamiento de datos se incrementa (ver apartado 8). Se permite el envío de mensajes publicitarios o comerciales por correo electrónico a aquellos usuarios que previamente lo hubieran solicitado o autorizado de forma expresa. También se admite el envío de comunicaciones comerciales a aquellos usuarios con los que exista una relación contractual previa, en cuyo caso el proveedor podrá enviar publicidad sobre productos o servicios similares a los contratados por el cliente.

18

'Cookies'

Si la empresa dispone de una página web, es probable que utilice *cookies*, que son unos pequeños ficheros que almacenan información del usuario que accede a la web (como, por ejemplo, información sobre los hábitos de navegación de ese usuario para después enviarle publicidad personalizada). Pues bien, la ley obliga a informar a los usuarios y obtener su consentimiento para utilizar o instalar *cookies*, y prevé sanciones importantes en caso de incumplimiento. No deberá cumplir esa obligación la web que sólo utilice *cookies* técnicas, que sirven para que la web se cargue correctamente, o *cookies* necesarias para prestar un servicio solicitado por el usuario (como el carrito de la compra virtual).

19

Reclamaciones

Si un interesado ejercita alguno de los derechos del apartado 13, el organismo está obligado a contestarle en el plazo de un mes, aunque no tenga datos suyos. Y en caso de no dar curso a su solicitud, deberá informarle de la posibilidad de presentar una reclamación ante la AEPD y de ejercitar acciones judiciales. El RGPD otorga el derecho a toda persona que haya sufrido daños y perjuicios (materiales o inmateriales) como consecuencia de una infracción del Reglamento a reclamar una indemnización ante los tribunales sin perjuicio de su derecho a presentar una denuncia ante la AEPD.

20

Páginas web

Si se tiene una página web meramente informativa, que se utiliza como escaparate virtual de los productos o servicios que ofrece una empresa pero con la que no capta datos personales, el RGPD no resultará de aplicación. Ahora bien, la cosa cambia –y deberá tenerse en cuenta esta norma necesariamente– si la página web incluye un campo en el que solicita la dirección electrónica de los usuarios del sitio (para enviarles un boletín de noticias, catálogos, etc.). También queda concernida si incluye un formulario de contacto que los usuarios tienen que completar para, por ejemplo, enviar consultas. A su vez, en el caso de que permita la compraventa en línea de sus productos o servicios, para lo cual los usuarios tienen que facilitar sus datos personales. En todos estos casos, se estará obteniendo datos personales de los usuarios de la página web, por lo que es necesario que se inserte un aviso legal para dar cumplimiento al deber de información y consentimiento. Es necesario que los usuarios acepten expresamente dicho aviso.