GUÍA

SOBRE NOVEDADES EN **PROTECCIÓN DE DATOS:**

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS
Y LEY ORGÁNICA DE PROTECCIÓN DE DATOS
Y GARANTÍA DE LOS DERECHOS DIGITALES

CONFEDERACIÓN CANARIA DE EMPRESARIOS
CEOE CEPYME

Gobierno de Canarias
Consejería de Empleo, Políticas Sociales y Vivienda

CONFEDERACIÓN CANARIA DE EMPRESARIOS

CEOE CEPYME

Gobierno de Canarias

Consejería de Empleo, Políticas Sociales y Vivienda

Este manual ha sido elaborado por la Confederación Canaria de Empresarios en el año 2018, en el marco de las diferentes actuaciones de Participación Institucional que desempeña esta Institución, y está financiada por la Consejería de Empleo, Políticas Sociales y Vivienda del Gobierno de Canarias.

Índice

Introducción

La Confederación Canaria de Empresarios, como organización empresarial más representativa que ostenta la representación institucional de los empresarios ante las Administraciones Públicas y organismos en el ámbito territorial de Canarias, al amparo de lo dispuesto en el párrafo primero de la Disposición adicional sexta del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores y la Ley 10/2014, de 18 de diciembre, de participación institucional de las organizaciones sindicales y empresariales más representativas de Canarias; según el criterio constitucional de irradiación por la pertenencia a las Confederaciones nacionales CEOE y CEPYME, así como por el reconocimiento asumido por el Gobierno de Canarias, de más representativa y de participación institucional, en el Acuerdo de la VI Mesa de Concertación Social Canaria (firmada el 25 de enero de 2018), y sobre la base del reconocimiento expreso de la Dirección General de Trabajo del Gobierno de Canarias, por informe escrito de fecha 5 de abril de 2016 y en el artículo 23.4 de la Ley Orgánica 1/2018, de 5 de noviembre, de reforma del Estatuto de Autonomía de Canarias, tiene como objetivo prioritario la defensa de los intereses empresariales de carácter general y la prestación de servicios a todos los sectores de actividad.

La Confederación Canaria de Empresarios es una organización empresarial sin ánimo de lucro, constituida el 12 de junio de 1978 al amparo de la Ley 19/1977, reguladora del Derecho de Asociación Sindical, con 40 años de antigüedad, basándose en un esquema de base sectorial y territorial, ha alcanzado, un alto grado de consolidación, notoriedad, reconocimiento, desarrollo y representatividad empresarial. Representa los intereses generales y comunes de las empresas sin distinción de tamaño, sector de actividad o ubicación, a través de un sistema único de integración asociativa, de unidad de acción empresarial y de no atomización de representaciones empresariales.

En este sentido, para poder desarrollar este acompañamiento al empresario canario, la Confederación Canaria de Empresarios, además de desempeñar su papel de máximo interlocutor social en los debates de transcendencia económica, respetado y valorado por todos los estamentos públicos, asume desde hace más de 20 años la prestación de una serie de servicios: Servicio Integral de Empleo para la creación de empresas y la orientación e inserción laboral, acciones de formación, así como actuaciones en materia de prevención de riesgos laborales, que funcionan de forma coordinada y cooperantes entre sí, con el fin último de prestar un servicio integral, activo y flexible que permita mejorar, tanto cuantitativa como cualitativamente, la situación del mercado laboral.

Dentro de toda esta labor, cobra especial relevancia la realización de proyectos durante los últimos años y los que pretende acometer en sucesivo dicha organización empresarial para la correcta adaptación de las empresas canarias a la legislación de protección de datos, ya que la correcta información y sensibilización sobre esta normativa resulta imprescindible para la protección de los derechos de los ciudadanos y la defensa de la buena marcha de la empresa.

Dentro del las actuaciones de Participación Institucional que desempeña esta institución, financiadas por la Consejería de Empleo, Políticas Sociales y Vivienda del Gobierno de Canarias, la Confederación Canaria de Empresarios ha elaborado este manual relativo a la legislación de protección de datos que ha entrado en vigor durante 2018: el Reglamento General de Protección de Datos, a nivel europeo, y la Ley Orgánica 3/2018, de 5 diciembre, de Protección de Datos y garantía de los derechos digitales, en España.

La protección de los datos personales, que, como veremos, ha sufrido un cambio de paradigma y ahora coloca a la empresa como principal garante de su ejecución y desarrollo, con el consiguiente aumento de responsabilidad y cargas, conlleva la necesidad de que éstas conozcan lo que la diferente normativa aplicable les exige, así como las herramientas y los derechos con los que cuentan para enfrentarse a la misma, así como las posibles sanciones para los casos en los que no fuera observada.

Estos aspectos han sido desarrollados en este documento con el fin de esbozar el contexto actual de esta problemática.

Capítulo 1. Reglamento (UE) 2016/679: Reglamento General de Protección de Datos.

Concepto

Nuevos principios

Nuevas definiciones

Concepto

El Reglamento General de Protección de Datos (RGPD) entró en vigor en mayo de 2016 y será aplicable a partir de mayo de 2018. Desde el inicio de su aplicación, el RGPD convivió con la entonces vigente Ley Orgánica de Protección de Datos (LOPD) y su Reglamento de Desarrollo, que posteriormente fueron sustituidas por la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. A pesar de la convencia de ambos cuerpos normativos, la Agencia Española de Protección de Datos (AEPD) recomendó encarecidamente a las organizaciones que traten datos de carácter personal ir preparando y adoptando las medidas necesarias para estar en condiciones de cumplir con las previsiones del RGPD desde el momento en el que sea de aplicación.

El RGPD, en tanto que no requiere de transposición, será de directa aplicación en todo el territorio de la Unión Europea a partir del 25 de mayo de 2018. Esto significa que el RGPD sustituirá la normativa nacional como marco jurídico de referencia, aunque las diferentes leyes nacionales podrán incluir algunas precisiones o desarrollos en materias en las que el RGPD lo permita.

La norma europea se aplica al tratamiento total o parcialmente automatizado de datos personales de las personas físicas y persigue su protección en lo que respecta al tratamiento de los datos personales. Regula también las normas relativas a la libre circulación de estos datos, esgrimiendo los derechos y libertades fundamentales de las personas físicas como el objeto a proteger, e incluye en su ámbito de aplicación a todas las organizaciones que ofrezcan bienes y servicios y manejen datos de ciudadanos de la Unión Europea, con independencia de su localización.

En resumidas cuentas, el Reglamento moderniza la normativa actual y unifica todo lo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos entre los Estados miembros.

A diferencia del sistema anterior, en el que cada país contaba con sus propias normas de protección de datos de aplicación a nivel nacional, y que implica para las empresas enfrentarse a una maraña de normas y gastos de asesoría jurídica, la norma europea pasa a homogeneizar la normativa de protección de datos para todo el territorio del Espacio Económico Europeo. Se espera que la creación de un marco único para todos facilite la igualdad de tratamiento, aumentando las opciones de negocio para las PYMES que podrán sacar el máximo partido a un mercado único digital.

Aunque el RGPD contiene modificaciones de algunos aspectos del régimen de protección de datos vigente a fecha de su entrada en vigor y contiene nuevas obligaciones para los responsables del tratamiento, también mantiene muchos conceptos principios y mecanismos establecidos en la LOPD. Es por esto que las organizaciones que en la actualidad cumplen con la normativa española tienen una buena base para una transición sin sobresaltos a lo dispuesto en el nuevo Reglamento, y no deberían incurrir en una mayor carga de trabajo en lo que respecta al tratamiento de datos personales, aunque si un mayor compromiso en su protección.

Nuevos principios

Dos son las principales novedades del RGPD: el principio de responsabilidad proactiva, que es descrito en la norma como la necesidad de que el responsable de tratamiento "aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento"; y el enfoque de riesgo, que llama a tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas cuando se adopten medidas dirigidas a garantizar su cumplimiento.

El RGPD introduce también por primera vez la figura del Delegado de Protección de Datos (DPD), que será obligatorio para algunas organizaciones en función de su naturaleza o actividades que realicen. Son novedades también la aplicación del principio de transparencia en la protección de datos, que llama a la simplificación del acceso y comunicación de la información a los interesados; y la necesidad de que el consentimiento sea inequívoco, es decir, otorgado mediante acción afirmativa por el interesado.

A la hora de aplicar las medidas previstas en el RGPD, las organizaciones deberán tener en mente el enfoque de riesgo, pues éstas pueden ser solo necesarias cuando exista un riesgo alto para los derechos y libertades de los interesados (como por ejemplo la evaluación de impacto del tratamiento de datos) o deben ser moduladas en función del nivel y tipo de riesgo que los tratamientos presenten: lo que puede ser adecuado para una organización que maneje datos de millones de interesados, o datos sensibles, con numerosas operaciones de tratamiento, no puede ser necesario para una pequeña empresa que lleva a cabo un volumen pequeño de operaciones simples de tratamiento de datos no sensibles.

Nuevas definiciones

El RGPD también amplía las definiciones de ciertos elementos claves en la protección de datos:

- Datos personales: toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Incluye también los datos de contacto, hasta ahora excluidos de la normativa de protección de datos.
- Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
- Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.
- Responsable del tratamiento o responsable: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.
- Encargado del tratamiento o encargado: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
- Violación de la seguridad de los datos personales: toda violación de la seguridad que 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.

Capítulo 2. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El pasado 6 de diciembre de 2018, se publicó en el Boletín Oficial del Estado (BOE) la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

Esta nueva ley, nacida de la adaptación de la normativa nacional al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (conocido también como Reglamento General de Protección de Datos o RGPD), sustituye a la anterior Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Cabe recordar que dicho Reglamento entró en vigor el pasado 25 de mayo de 2018 y, cómo anunció la Agencia Española de Protección de Datos (AEPD), es de obligatorio cumplimiento de forma automática para todas las empresas que operen dentro de la Unión Europea.

La nueva ley orgánica, así como el RGPD, responden a nuevas circunstancias enumeradas en el preámbulo de la LOPDGDD: necesidad de una regulación más uniforme en el marco de una sociedad cada vez más globalizada; el aumento de los flujos transfronterizos de datos personales; la evolución tecnológica y globalización; la aparición de nuevos servicios y productos relacionados con los datos personales, y su comercialización; los nuevos riesgos; y la mayor accesibilidad y procesamiento de los datos de carácter personal, que requieren una mayor protección. Todas estas circunstancias están estrechamente relacionadas con la preminencia de internet en nuestras vidas, herramienta que se ha convertido indispensable en nuestra actividad profesional, económica y privada y que acarrea riesgos y oportunidades específicas que requieren de una regulación adaptada a los nuevos desafíos.

La LOPDGDD se compone de 97 artículos estructurados en 10 títulos, 22 disposiciones adicionales, 6 disposiciones transitorias, una disposición derogatoria y 16 disposiciones finales. Aunque el texto reproduce en gran medida los preceptos introducidos en el RGPD, contiene una serie de novedades que pasamos a comentar a continuación:

- El Título III, dedicado a los derechos de las personas y que reproduce y complementa los derechos tradicionales en materia de protección de datos (derechos ARCO y los nuevos derechos de limitación al tratamiento y supresión), se completa con la introducción de nuevos derechos digitales en el Título X (artículos 79 a 97): derecho a la neutralidad de Internet; derecho de acceso universal a Internet; derecho a la educación digital; derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral; derecho a la desconexión digital en el ámbito laboral; derechos digitales en la negociación colectiva; o derecho al testamento digital.

- La ejecución de estos derechos lleva al llamamiento que hace la LOPDGGD de incluir en el currículum académico la formación del alumnado en el uso seguro y adecuado de internet, quedando los detalles de esta inclusión a posterior desarrollo legal.
- Se elevan las cuantías de las sanciones asociadas a cada tipo de infracción, llegando a 20 millones de euros en los casos más graves. En materia sancionadora, y en los casos en los que la Administración sancione a un ciudadano, la publicación de dicha sanción en anuncios para los casos en que no se pudiera notificar al interesado solo podrá contener, como identificación, el nombre y cuatro cifras aleatorias del D.N.I., minimizando el potencial impacto negativo de esta publicación.
- El Delegado de Protección de Datos pasa a tener nuevas y ampliadas funciones, a la vez que se introduce un listado de entidades que deberán contar de forma obligatoria con esta figura. Se recoge también el papel de intermediador del delegado en los casos de reclamación ante las autoridades de protección de datos.
- La inclusión en los llamados ficheros de morosos será solo posible con una deuda superior a los 50 euros, elevando la cantidad desde los un euros anteriores, y reducen de 6 a 5 años el período máximo de inclusión de las deudas.
- Se fija en 14 años la edad mínima para prestar el consentimiento de manera autónoma, regulando también el ejercicio de sus derechos.
- Regula de forma explícita el tratamiento de los datos de contacto de empresarios individuales y de profesionales liberales, y plasma que este tratamiento es lícito al perseguir el interés legítimo del responsable del tratamiento.
- Introduce regulación expresa acerca de los sistemas de información de denuncias internas, esenciales en los sistemas de compliance de las empresas, haciéndose eco del principio de confidencialidad que debe imperar en el proceso y siguiendo el criterio de la AEPD plasmado en su informe nº 128/2007.
- La disposición final tercera de la LOPDGDD introduce la posibilidad de que los partidos políticos recojan y utilicen los datos personales de terceros para llevar a cabo sus actividades electorales. Esta inclusión ha sido matizada por la AEPD y cuestionada en su adecuación a la normativa europea por algunos colectivos, partidos políticos y representantes de instituciones europeas.
- Por último, y como resultado de la necesidad de adaptación a un nuevo marco normativo de protección de datos, se regulan como prácticas de competencia desleal la suplantación de la identidad de la AEPD y las prácticas relacionadas con la llamada “adaptación a coste cero”, con el fin de limitar la oferta de asesoramientos de ínfima calidad a empresas.

Las novedades que acabamos de enumerar conllevan la modificación de importantes leyes, como el texto refundido de la Ley del Estatuto de los Trabajadores y de la Ley del Estatuto Básico del Empleado Público; la Ley Orgánica 5/1985, de 19 de Junio, del Régimen Electoral General; la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas; la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno; Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial; la Ley 14/1986, de 25 de abril, General

de Sanidad; o la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa; a cuya nueva redacción habrá que estar atentos.

Capítulo 3. Legitimación para el tratamiento de datos.

Legitimación para el tratamiento de datos.

El RGPD mantiene que todo tratamiento de datos necesita estar respaldado por una base que lo legitime. Manteniendo los preceptos ya existentes en la anterior LOPD, las bases jurídicas que autorizan al tratamiento de datos son las siguientes:

- Consentimiento.
- Relación contractual.
- Intereses vitales del interesado o de otras personas.
- Obligación legal para el responsable.
- Interés público o ejercicio de poderes públicos.
- Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

La novedad introducida por el RGPD es la necesidad de informar a los interesados de la base jurídica por la que sus datos van a ser tratados. Así, como se verá más adelante, la base legal sobre la que se desarrolla el tratamiento deberá ser incluida al proporcionar la información en el momento de recoger los datos de los interesados, especificando y documentando los intereses legítimos en que se fundamentan las operaciones de tratamiento.

La identificación de la base legal por la que se lleva a cabo el tratamiento de los datos personales es indispensable para poder demostrar el cumplimiento de las previsiones del RGPD.

La identificación de la finalidad del tratamiento de datos supone la segunda parte necesaria para considerarlo legítimo. El RGPD establece la necesidad de identificar con precisión las finalidades y la base jurídica de los tratamientos que lleva a cabo la empresa, requiriendo recabar el consentimiento del interesado para cada una de las distintas finalidades. Se exige que, si en el futuro el responsable del tratamiento pasa a usar la información para una finalidad distinta, se deberá informar a los interesados.

La identificación de finalidades y base jurídica tiene exigencias adicionales en los casos en que se traten datos de especial protección como los relacionados con salud, ideología, religión o pertenencia étnica, pues su tratamiento está, con carácter general, prohibido y solo podrá llevarse a acabo si recae en alguna de las excepciones previstas en el Reglamento y con consentimiento expreso del interesado.

La LOPDGGD ha optado por regular una situación que había generado ciertas dudas: el tratamiento de los datos de contacto de empresarios individuales o profesionales liberales. El artículo 19 da la posibilidad de que estos datos se traten de forma legítima basándose en el interés legítimo del responsable o del tercero, sin necesidad de recabar consentimiento previo, pero limitando este tratamiento a los datos de contacto y en el marco de una relación profesional.

Capítulo 4. Consentimiento.

Consentimiento

Consentimiento en caso de menores

Consentimiento.

El RGPD introduce la necesidad de que el consentimiento sea otorgado de forma inequívoca, descartando formas de consentimiento tácito o por omisión como justificación para el tratamiento de datos, e incluso requiriendo la obtención de consentimiento explícito para el tratamiento de ciertos datos.

El consentimiento inequívoco es aquel que se ha prestado mediante la manifestación del interesado o mediante una clara acción afirmativa. Aunque el consentimiento tácito pasa a ser derogado, el consentimiento puede ser inequívoco y otorgado de forma implícita cuando se deduzca de una acción del interesado (continuar navegando por una página web, aceptando así las cookies, es un ejemplo). En todo caso, el responsable deberá probar que cuenta con el consentimiento del interesado y que ha sido prestado a través de los medios pertinentes.

El RGPD introduce además casos en los que el consentimiento deber ser no solo inequívoco, pero también explícito:

- Tratamiento de datos sensibles.
- Adopción de decisiones automatizadas (elaboración de perfiles).
- Transferencias internacionales.

En cualquier caso, no se podrá seguir obteniendo el consentimiento por omisión (mediante casillas premarcadas, por ejemplo) o tácito, y se llama a las organizaciones a revisar sus políticas de obtención de datos para que se adecúen a los preceptos del RGPD. Esta adaptación puede llevarse a cabo mediante:

- Obtención de un nuevo consentimiento de los interesados acorde con las disposiciones del RGPD.
- Valorando si los tratamientos de datos afectados pueden apoyarse en otra base legal (diferente legitimación del tratamiento).

Cuando se preste el consentimiento para el tratamiento de datos con múltiples finalidades será preciso dar el consentimiento para todas ellas. Sería posible, por otro lado, agrupar las finalidades en virtud de su vinculación, y por lo tanto, recabar un único consentimiento; pero deberá ser desagregado cuando los tratamientos impliquen conductas distintas.

Ejemplo: para garantizar que el consentimiento es inequívoco, se recomienda la inclusión en los formularios online de casillas en las que el interesado marca y confirma que ha leído la política de privacidad.

Para convertir los consentimientos tácitos obtenidos con anterioridad a la entrada en vigor del RGPD en consentimientos inequívocos, se recomienda solicitar a los interesados la renovación del mismo. Esto se puede hacer, por ejemplo, con una invitación a ser incluidos en una lista de mailing en la que deberán aceptar la política de privacidad de la organización, asegurando así la acción afirmativa requerida en la norma.

Datos sensibles: origen étnico o racial; opiniones políticas; convicciones religiosas o filosóficas; afiliación sindical; datos genéticos; datos biométricos; datos relativos a la salud o a la vida sexual; y la orientación sexual.

Consentimiento en caso de menores.

El RGPD hace referencia expresa en varios preceptos al tratamiento de los datos de los menores. Esta mención explícita está relacionada con la obtención del consentimiento, que, en el caso de la oferta de servicios de la sociedad de la información, solo será válido a partir de los 16 años.

Con anterioridad a los 16 años, el consentimiento otorgado deberá contar con la autorización de los padres o tutores legales. En cualquier caso, el Reglamento permite a los estados miembros establecer una edad inferior, siempre que no sea menor de 13 años. Con la introducción de la nueva normativa de protección de datos española, la edad de consentimiento en España se ha rebajado a los 14 años.

El RGPD requiere que los responsables hagan esfuerzos razonables para verificar que el consentimiento se ha dado por un mayor de 16 años o con autorización de los padres o tutores del menor. No es una obligación en sí, sino la necesidad de que las organizaciones establezcan medios, en función de la tecnología disponible, para garantizar la intervención real de padres y tutores.

Capítulo 5. Nuevos derechos y deberes.

Deber de información

Derecho de acceso

Derecho a la supresión o al olvido

Derecho a la limitación del tratamiento

Derecho a la portabilidad de los datos

Derecho de acceso universal a internet

Derecho a la seguridad digital

Derechos de los trabajadores en la LOPDGGD

Procedimiento para el ejercicio de los derechos

Nuevos derechos y deberes.

Los derechos de acceso, rectificación, consulta y oposición (derechos ARCO), actualmente contemplados tanto en la normativa europea como nacional, se ven extendidos por el RGPD. Por otro lado, se introducen los derechos a la supresión, limitación del tratamiento y portabilidad de los datos a partir del 25 de mayo de 2018.

Del mismo modo, la aplicación del RGPD y sus requisitos de transparencia traerán nuevas obligaciones para las organizaciones, que deberán proporcionar la información sobre el tratamiento de los datos del interesado de forma concisa, inteligible y de fácil acceso.

Deber de información.

El RGPD trata de alejar las fórmulas farragosas y remisiones a cuerpos legales a la hora de informar a los interesados del tratamiento de sus datos y sus derechos. Mientras que la LOPD exigía que la información se preste de modo expreso, preciso e inequívoco, el Reglamento establece que la información a los interesados deberá proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. En consecuencia, los procedimientos, modelos o formularios diseñados de acuerdo con la antigua LOPD deberán ser revisados y adaptados incorporando los nuevos requisitos de transparencia.

Las cláusulas informativas deberán explicar el contenido al que inmediatamente se refieren de forma clara y accesible para los interesados, y contener como mínimo:

- Base jurídica o legitimación del tratamiento.
- Intención de realizar transferencias internacionales.
- Datos del Delegado de Protección de Datos (si lo hubiere).
- Elaboración de perfiles o existencia de decisiones automatizadas.
- El derecho a presentar una reclamación ante las Autoridades de Control.
- El plazo o los criterios de conservación de la información.
- En el caso de que los datos no hayan sido obtenidos directamente del propio interesado:
- El origen de los datos.
- Las categorías de los datos.

Esta información se deberá poner a disposición de los interesados en el momento en que se soliciten los datos, previamente a la recogida o registro, y si no se obtuvieran directamente del interesado, dentro de un plazo razonable. Se exceptúa del deber de informar los casos en los que el interesado ya disponga de la información, o cuando los datos no procedan del interesado y la comunicación resulte imposible o suponga un esfuerzo desproporcionado; la comunicación esté expresamente establecida en la normativa; o cuando los datos deban seguir teniendo carácter confidencial por imperativo legal.

En cuanto a las formas de informar a los interesados, son tan variadas como formas de obtener la información existen. Algunas de las formas más habituales son formularios en papel, formularios web, entrevista telefónica, registro de aplicaciones móviles, correo postal, mensajería electrónica o notificaciones emergentes en servicios y aplicaciones. En cualquier caso, la información a las personas interesadas debe proporcionarse con un lenguaje claro y sencillo, y de forma concisa, transparente, inteligible y de fácil acceso.

Para facilitar a los responsables del tratamiento adaptarse a las nuevas exigencias del RGPD, se ha establecido un modelo de información por capas o niveles: un primer nivel con la información básica, de forma resumida, proporcionada en el mismo momento y medio en el que se recojan los datos; y un segundo nivel en el que se remita a la información adicional, donde se presentarán detalladamente el resto de las informaciones. A continuación, se presenta un ejemplo de estas capas y resumen de los contenidos que deberán tener:

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Responsable" (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
"Finalidad" (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
"Legitimación" (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.
		Obligación o no de facilitar datos y consecuencias de no hacerlo
"Destinatarios" (de cesiones o transferencias)	Previsión o no de Cesiones	Destinatarios o categorías de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
"Derechos" (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de Control
"Procedencia" (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

Fuente: "Guía para el Cumplimiento del Deber de Informar". AEPD.

Primera capa de información

El epígrafe "legitimación" hace referencia a la base jurídica en la que se basa el tratamiento, que atendiendo al RGPD deberá estar entre las siguientes opciones:

- Ejecución de un contrato.
- Cumplimiento de una obligación legal.
- Misión en interés público o ejercicio de poderes públicos.
- Interés legítimo del responsable o de un tercero.
- Consentimiento del interesado.

En el caso de que un tratamiento persiga varias finalidades, se hará constar la legitimación para la finalidad principal del tratamiento.

El epígrafe de "destinatarios" facilita a los interesados una mejor comprensión del tratamiento, y deberá aparecer aún cuando no se prevea la comunicación de los datos personales a terceros.

El epígrafe "derechos" también debe aparecer siempre en la información básica. Se recomienda hacer una breve alusión a la existencia de los derechos más habituales y referencia al epígrafe correspondiente en la información adicional.

Por último, deberá incluirse dónde y cómo puede acceder el interesado a la información adicional en la segunda capa; y en el caso de que los datos no hayan sido obtenidos directamente del interesado, se tendría que añadir la procedencia de estos.

Se recomienda que la primera capa presente la información en forma de tabla, de manera análoga a como se presenta la información nutricional alimentaria, garantizando que dicha información quede a simple vista del interesado e identificada con un título como "Información básica sobre protección de datos". Por ejemplo:

INFORMACIÓN BÁSICA DE PROTECCIÓN DE DATOS

RESPONSABLE	Empresa X
FINALIDAD	Gestionar envío
LEGITIMACIÓN	Ejecución de un contrato
DESTINATARIOS	Otras empresas del grupo empresarial X, S.A.
DERECHOS	Acceder, rectificar y suprimir los datos, así como otros derechos recogidos en la información adicional
INFORMACIÓN ADICIONAL	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web: www.empresax.es/protecciondatos/

Segunda capa de información

La información que se presente en la segunda capa ha de completar con todos los detalles la información resumida en la primera capa, así como añadir la información adicional requerida por el RGPD. Su presentación dependerá del medio empleado para informar, ofreciendo una mayor flexibilidad en su presentación y extensión.

- Tras ofrecer la identidad del responsable del tratamiento en la primera capa, en la segunda se deberá completar su información mediante la incorporación de sus datos de contacto y, en su caso, de su representante; y los datos de contacto del Delegado de Protección de Datos si lo hubiera. Se recomienda proporcionar una dirección postal y una dirección electrónica o link a formulario de contacto electrónico. Por ejemplo:

¿Quién es el responsable del tratamiento de sus datos?

Identidad: Empresa X, S.A. – CIF: A01234567
Dirección postal: Calle Valverde, S/N – 35000 – Las Palmas
Teléfono: 928123456
Correo electrónico: info@empresax.es
Delegado de Protección de Datos: José García
Contacto DPD: jg@empresa.es o www.empresax.es/protecciondatos/dpd

- En esta segunda capa deberá informarse con mayor detalle de los fines del tratamiento a que se destinan los datos personales, incluyendo el plazo durante el cual se conservarán los datos, o, si no se conociera, los criterios que se utilizarán para determinarlo. Del mismo modo, se

deberá informar al interesado de la existencia de decisiones automatizadas, incluida la elaboración de perfiles, y se detallará la lógica aplicada, la importancia y las consecuencias previstas de dicho tratamiento para el interesado. Por ejemplo:

¿Con qué finalidad tratamos sus datos personales?
En Empresa X tratamos la información que nos facilitan las personas interesadas con el fin de gestionar el envío de los productos que nos soliciten y facilitar a los interesados ofertas de productos y servicios de su interés. Con el fin de poder ofrecerle futuros productos y servicios de acuerdo con sus intereses, elaboraremos un perfil comercial en base a la información facilitada. No se tomarán decisiones automatizadas en base a dicho perfil. ¿Por cuánto tiempo conservaremos sus datos? Los datos personales proporcionados se conservarán hasta que no se solicite su supresión por el interesado, y en todo caso, mientras se mantenga la relación mercantil.

- El epígrafe legitimación deberá introducir referencia específica a la base jurídica por la cual se tratan los datos personales. En el caso de ejecución de contrato, se deberá hacer mención del contrato o tipo de contrato de que se trate; en el caso de obligación legal o interés público, se deberá hacer constar cuál es la norma que impone la obligación; en el caso de que el tratamiento se base en el interés legítimo del responsable o de un tercero, se deberá especificar cuáles son los intereses, incluyendo una ponderación de la legitimidad frente a los intereses y derechos y libertades del individuo; y por último, si la base del tratamiento es el consentimiento, se deberá especificar si la finalidad principal está legitimada por alguna de las otras bases jurídicas y el consentimiento solo se requiere para alguna finalidad específica, debiendo constar ambas legitimaciones. Por último, cabe mencionar que, si la comunicación de datos personales es un requisito legal o contractual, deberá informarse de si el interesado está obligado a facilitar los datos personales y las consecuencias en el caso de que no acceda a ello.

¿Cuál es la legitimación para el tratamiento de sus datos?
La base legal para el tratamiento de sus datos es la ejecución del contrato de envío de los productos de Empresa X que figuran en su cartera de pedidos. La oferta prospectiva de productos y servicios está basada en el consentimiento que se le solicita, sin que en ningún caso la retirada de este consentimiento condicione la ejecución del contrato de envío.

- Cuando se prevea comunicar los datos personales que se recogen, se deberá informar acerca de la identidad de los destinatarios. En particular, se recomienda informar también de la existencia de encargados de tratamiento, cuya legitimidad del tratamiento es la ejecución del contrato de encargo. Cuando se prevea transmitir datos personales a terceros países u organización, se deberá informar a los interesados de las condiciones de estas transferencias y de la existencia o ausencia de una decisión de adecuación de la Comisión respecto al destino. En el caso de que la transferencia se realice con el aporte de garantías adecuadas o

apropiadas por parte del responsable, se deberá también informar de las mismas y los medios para obtener una copia de éstas.

¿A qué destinatarios se comunicarán sus datos?
Los datos se comunicarán a otras empresas del grupo empresarial X, S.A. para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados; y para fines de promoción y oferta de productos y servicios del grupo empresarial X, S.A.

- La información adicional sobre los derechos de los interesados deberá contener información sobre los derechos que les asisten (acceso, rectificación, supresión, limitación, oposición, portabilidad), así como información clara sobre cómo se pueden ejercer estos derechos, mediante la puesta a disposición de los interesados de un modelo o formulario y los datos de contacto para formular su solicitud. Por último, deberá informar de que el interesado tiene derecho a retirar el consentimiento y a presentar una reclamación ante la autoridad de protección de datos competente.

¿Cuáles son sus derechos cuando nos facilita sus datos?
Cualquier persona tiene derecho a obtener confirmación sobre si en Empresa X estamos tratando datos personales que les conciernan, o no. Las personas interesadas tienen derecho a acceder a sus datos personales, así como a solicitar la rectificación de los datos inexactos, o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos. En determinadas circunstancias, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones. (…)

- La información sobre la procedencia de los datos solo habrá de incluirse cuando éstos no hayan sido obtenidos directamente del interesado, por proceder de alguna cesión legítima o de acceso público.

¿Cómo hemos obtenido sus datos?
Los datos personales que tratamos en Empresa X proceden de otras empresas del grupo empresarial X, S.A. Las categorías de datos que se tratan son: • Datos de identificación. • Códigos o claves de identificación. • Direcciones postales y electrónicas. • Información comercial. • Datos económicos. No se tratan datos especialmente protegidos.

La AEPD, con la colaboración de las autoridades de protección de datos de Cataluña y el País Vasco, ha elaborado una Guía para el Cumplimiento del Deber de Informar, que detalla y ofrece más ejemplos sobre como comunicar la información requerida en el RGPD a los interesados.

Los ejemplos aquí proporcionados no contemplan todos los supuestos y no agotan las posibilidades de información, por lo que no deben tomarse como un modelo aplicable a cualquier tratamiento sino como un posible estilo de información en unos casos concretos y con la información mínima que debiera ofrecerse.

Derecho de acceso.

Aunque ya contemplado en la actual normativa, el RGPD lo amplia y recoge el derecho de los interesados a obtener una copia de los datos personales objeto de tratamiento. Este derecho se podrá atender a través del acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales.

Derecho a la supresión o al olvido.

El interesado tendrá derecho a obtener la supresión de sus datos en el caso que éstos ya no sean necesarios en relación con los fines para los que fueron recogidos; cuando retire su consentimiento para el tratamiento; o cuando éstos hayan sido tratados ilícitamente.

Según el Tribunal de Justicia Europeo, el derecho al olvido no es un derecho autónomo sino una manifestación de los derechos de cancelación u oposición en el entorno online. Los responsables que apliquen en la actualidad esta jurisprudencia no tienen que introducir ninguna modificación en sus prácticas, aunque si deberán introducir medidas técnicas adecuadas para informar a otros responsables de la solicitud del interesado de borrar su información personal si la han hecho pública.

La LOPDGG dedica dos artículos al derecho al olvido, tanto en búsquedas de internet como en servicios de redes sociales.

El artículo 93 contiene el derecho de las personas a que los motores de búsqueda de internet eliminen de las listas de resultados obtenidas de una búsqueda de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuese inadecuada, inexacta, no pertinente, no actualizada o excesiva o hubieran devenido como tal por el transcurso del tiempo. Este derecho estará limitado al acceso a la información pertinente a través de la búsqueda de otros criterios distintos al nombre, por lo que la información podrá seguir siendo accedida a través de otras palabras clave.

Por su parte, el derecho al olvido en servicios de redes sociales y servicios equivalentes permite a cualquier persona solicitar la supresión, con una simple solicitud, de los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y otros equivalentes.

Este derecho se ve ampliado por la posibilidad de solicitar la supresión de información publicada por terceros siempre que ésta sea inadecuada, inexacta, no pertinente, no actualizada o excesivo o hubiese devenido como al por el paso del tiempo. Igualmente, en el caso de menores, se procederá a la supresión de esta información sin que medien ninguna de las circunstancias anteriormente mencionadas, bastando la simple solicitud.

Derecho a la limitación del tratamiento.

Supone el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro. Mientras dure la limitación, el responsable sólo podrá tratar los datos afectados, más allá de su conservación, con el consentimiento del interesado; para la formulación, el ejercicio o la defensa de reclamaciones; para proteger los derechos de otra persona física o jurídica; o por razones de interés público importante de la Unión o del Estado miembro correspondiente.

El interesado tendrá derecho a obtener la limitación del tratamiento de sus datos cuando, por ejemplo, impugne la exactitud de los datos personales; cuando el tratamiento sea ilícito; o cuando el responsable ya no necesite los datos para los fines del tratamiento.

Derecho a la portabilidad de los datos.

El interesado podrá solicitar del responsable de tratamiento el envío de un archivo con sus datos; o la transmisión de éstos a otro responsable del tratamiento.

Este derecho solo puede ejercerse cuando el tratamiento se efectúe por medios mecánicos; se base en el consentimiento o en un contrato; y cuando el interesado lo solicita respecto a los datos que haya proporcionado al responsable y que le conciernan. En cualquier caso, este derecho no puede ejercerse sobre los datos de terceras personas que un interesado haya facilitado a un responsable; o en el caso de que el interesado haya solicitado la portabilidad de datos que le incumban pero que hayan sido proporcionados al responsable por terceros.

La copia que se proporciona al interesado debe ofrecerse en un formato estructurado, de uso común y de lectura mecánica.

La LOPDGGD, en su artículo 95, incluye una mención específica al derecho de portabilidad en servicios de redes sociales, abriendo la puerta a que los usuarios de dichas redes puedan recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que estos los transmitan a otro prestador designado por el usuario y siempre que sea técnicamente posible.

Derecho de acceso universal a internet.

Se garantiza el acceso universal, asequible y de calidad y sin discriminación a internet para toda la población. El objetivo principal de esta medida es reducir, y potencialmente superar, la brecha de género y generacional, tanto en el ámbito personal como laboral, mediante acciones dirigidas a la formación y el acceso a internet, con especial atención a entornos rurales y personas con necesidades especiales.

Derecho a la seguridad digital.

Se garantiza el derecho de los usuarios a la seguridad de las comunicaciones que transmitan y reciban a través de internet. De igual manera, se llama a los proveedores de servicios de internet a informar a los usuarios de sus derechos.

Derecho a la educación digital.

Con la introducción de este derecho, el sistema educativo deberá garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con los valores constitucionales, los derechos fundamentales y la garantía de la intimidad personal y familiar y la protección de datos personales.

Para logar la consecución de este mandato legal, las administraciones educativas habrán de incluir entre las asignaturas de libre configuración esta educación digital, así como elementos relacionados con situaciones de riesgo resultado de la inadecuada utilización de las TIC. En cuanto a la enseñanza universitaria, los planes de estudios de los títulos universitarios deberán incluir formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en internet, especialmente aquellos que habiliten para para la formación del alumnado.

El profesorado deberá recibir también la formación necesaria en competencias digitales, garantizando la adecuada enseñanza y transmisión de los valores y derechos anteriores. En el caso de procesos de selección de empleados públicos, la Administración deberá incluir a los temarios de estas pruebas materias relacionadas con la garantía de derechos digitales y la protección de datos, especialmente para procesos de acceso a los cuerpos superiores y los que desempeñen funciones que impliquen el acceso a datos personales.

Derechos de rectificación en internet y actualización de informaciones en medios de comunicación digitales.

El artículo 85 LOPDGGD, tras proclamar la libertad de expresión en internet, llama a los responsables de redes sociales y servicios equivalentes a adoptar los protocolos adecuados que permitan a los usuarios el ejercicio del derecho de rectificación ante contenidos que atenten contra sus derechos al honor, la intimidad personal y familiar en internet, o a recibir libremente información veraz.

Este derecho de rectificación será de aplicación también a los casos en los que la información aparezca en medios de comunicación digitales. En el caso de que sea un medio de comunicación el que tenga que atender una solicitud de rectificación, nos dice el artículo 86 que deberá también publicar en sus archivos digitales de un aviso aclaratorio que manifieste que la noticia original no refleja la situación actual del individuo, en un lugar visible junto con la información original. Esta rectificación será especialmente relevante cuando la información original se refiere a actuaciones policiales o judiciales que hayan resultado en beneficio del interesado como consecuencia del desarrollo de las acciones judiciales o policiales.

Derechos al testamento digital.

El artículo 96 regula el acceso a los contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas o, como comúnmente se denomina, el testamento digital, es decir, los datos personales e información del fallecido.

El acceso a estos datos se podrá realizar por familiares del fallecido o herederos, que deberán contactar con el prestador del servicio para acceder a la información e impartir las instrucciones que estimen oportunas sobre su utilización, destino o supresión; el albacea testamentario, siguiendo las instrucciones recibidas; los representantes legales o el Ministerio Fiscal en el caso de menores; o, en el caso de personas con discapacidad, por sus representantes legales, el Ministerio Fiscal o aquellos designados para el ejercicio de funciones de apoyo.

Entre las medidas que podrán tomar las personas anteriormente enumeradas, están el mantenimiento o eliminación de los perfiles personales de las personas fallecidas. Sus acciones estarán, en todo caso, limitadas por lo deseado por la persona fallecida (si dejara constancia de ello) o si lo hubiera prohibido de forma expresa.

Se deja a posterior legislación los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones, así como a competencia autonómica con derecho civil, foral o especial propio la regulación de este derecho.

Derechos de los trabajadores en la LOPDGGD

La publicación de la nueva normativa de protección de datos española incorporó al ordenamiento una serie de derechos y garantías digitales que afectan al ámbito de las relaciones laborales. En concreto, se introduce un artículo 20 bis al Estatuto de los Trabajadores que estipula los derechos de los trabajadores a la intimidad en relación con el entorno digital y la desconexión digital. Siguiendo el contenido del Título X de la LOPDGGD, se garantizan los siguientes derechos:

- Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, lo que supone la obligación para el empleador de establecer una serie de criterios de utilización de los dispositivos digitales con la única finalidad de controlar el cumplimiento de las obligaciones laborales por parte de sus empleados. Estos criterios deberán ser pactados con la representación legal de los trabajadores y respetar, en todo caso, el derecho a la intimidad de los empleados. Por ejemplo, se podrán fijar períodos durante los cuales pueda hacer uso personal de estas herramientas, etc.
- Derecho a la desconexión digital en el ámbito laboral, que tiene como objeto garantizar el respeto por parte del empleador del tiempo de descanso, permisos y vacaciones de los trabajadores, así como su intimidad familiar y personal. Para la salvaguarda de este derecho, se llama a los empleadores a elaborar, previa audiencia de los representantes de los trabajadores (ya sea en el marco de la negociación colectiva o de la empresa), una política interna que permita y module esta desconexión, así como que sensibilice a los empleados sobre el uso razonable de las tecnologías.
- Derecho a la intimidad frente al uso de dispositivos de video vigilancia y de grabación de sonidos en el lugar de trabajo, aunque se permite como hasta ahora el uso de estos sistemas para el ejercicio de las funciones de control de los trabajadores previstas en el art. 20.3 del Estatuto de los Trabajadores. Para ello, se deberá informar previamente de su instalación y características, así como su finalidad, y se deberá respetar en todo caso el derecho a la intimidad de los trabajadores, garantizando un uso proporcional y menos invasivo posible.
- Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral, que, como en el caso de los dispositivos de video vigilancia, deberá informarse a los empleados de su utilización, características y finalidad.
- Derechos digitales en la negociación colectiva, llamando a los convenios colectivos al establecimiento de garantía adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de sus derechos digitales.

Para la correcta observancia de estos derechos, la nueva LOPDGGD llama la implantación de nuevas políticas y protocolos y la actualización de los ya existentes, así como la definición y establecimiento de una estrategia en la negociación de estas políticas con los representantes de los trabajadores.

Procedimiento para el ejercicio.

Los responsables del tratamiento de datos deberán establecer procedimientos que permitan fácilmente a los interesados ejercer sus derechos. Se requiere que se facilite la presentación de solicitudes por medios electrónicos y la acreditación del ejercicio de estos derechos.

El ejercicio de estos derechos será gratuito para el interesado excepto en el caso de que se formulen peticiones manifiestamente infundadas o excesivas, especialmente por repetitivas. En este caso el responsable podrá cobrar un canon que compense los costes administrativos de tramitar la solicitud o negarse a actuar, pero deberá en todo caso demostrar el carácter infundado o excesivo de la solicitud y en ningún caso podrá obtener un beneficio a través de este canon.

El responsable cuenta con un mes para informar al interesado de las actuaciones derivadas de su petición o para informar al mismo de la negativa a su solicitud y los motivos para ello.

Por último, el ejercicio de las obligaciones inherentes a la actividad del responsable o encargado del tratamiento de datos también crea derechos para los interesados. Por ejemplo, el interesado tiene derecho a ser informado, en menos de 72 horas, de cualquier violación en los datos personales. Está notificación deberá ser clara, incluyendo las consecuencias de la violación y las medidas para poner remedio.

La AEPD ha elaborado una ficha con información sobre los derechos de los interesados y los requisitos para su ejercicio.

Capítulo 6. Relación responsable-encargado.

Relación responsable-encargado.

Tanto la normativa europea como las nacionales se han centrado tradicionalmente en la actividad de los responsables del tratamiento de datos. Aunque la responsabilidad última sobre el tratamiento de datos continúa estando sobre el responsable, el RGDP introduce obligaciones expresamente dirigidas a los encargados.

Los encargados pasan a tener obligaciones propias que no nacen del contrato que les une al responsable y que pueden ser supervisadas separadamente por las autoridades de protección de datos: deberán mantener un registro de actividades de tratamiento; determinar las medidas de seguridad aplicables a los tratamientos que realizan; y deben designar un DPD en los casos previstos. Del mismo modo, se contempla que los encargados puedan adherirse a códigos de conducta o certificarse como herramienta para demostrar su adecuación a la norma.

Por otro lado, el responsable pasa a tener el deber de tomar medidas apropiadas para garantizar y poder demostrar que el tratamiento de los datos se realiza de acuerdo con el RGPD, incluyendo entre estas medidas la elección del encargado. Así, se requiere que los responsables contraten solo con encargados que "ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas," de manera que el tratamiento sea conforme con los requisitos del Reglamento. En caso contrario, en un posible procedimiento sancionador, el responsable de tratamiento podría ser condenado por culpa "in vigilando" por las acciones del encargado, es decir, no sería responsable directamente, pero si indirecto por no haber tomado las debidas precauciones a la hora de formalizar un contrato con el encargado del tratamiento.

Por último, el RGPD recoge la necesidad de que las relaciones entre el responsable y el encargado se formalicen en un contrato o acto jurídico que vincule al segundo con el primero. Del mismo modo, el Reglamento regula minuciosamente el contenido mínimo de los contratos de encargo:

- Objeto, duración, naturaleza y la finalidad del tratamiento.
- Tipo de datos personales y categorías de interesados.
- Obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable.
- Condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones.
- Obligación del encargado de garantizar la seguridad del tratamiento.
- Asistencia al responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados y en garantizar la seguridad del tratamiento.
- Obligación del encargado de suprimir o devolver todos los datos personales una vez finalice la prestación de sus servicios.
- Obligación del encargado de poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el RGPD.

En el caso de contratos de encargo concluidos con anterioridad a mayo de 2018, éstos deberán modificarse y adaptarse para respetar el contenido listado.

La AEPD y las autoridades de protección de datos autonómicas han preparado unas directrices para la redacción de estos contratos, así como un modelo de cláusulas contractuales.

Capítulo 7. Principio de responsabilidad proactiva.

Principio de responsabilidad proactiva

Análisis del riesgo

Registro de actividades de tratamiento

Protección de datos desde el diseño y por defecto

Medidas de seguridad

Notificación de violaciones de seguridad de los datos

Evaluación de impacto sobre la protección de datos

Delegado de Protección de Datos (DPD)

Principio de responsabilidad proactiva.

El RGPD introduce este principio que, de forma resumida, podemos entender como la necesidad de que el responsable de tratamiento de datos aplique las medidas técnicas y organizativas apropiadas con el fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento. Este principio exige de las organizaciones una actitud consciente, diligente y proactiva frente a todos los tratamientos de datos personales que lleven a cabo.

En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, las finalidades con lo que lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento, deben determinar de forma explícita la forma en que aplicarán las medidas previstas en la norma, asegurándose de que éstas son las adecuadas para el cumplimiento del mismo y de que pueden demostrarlo ante las autoridades y los interesados.

Ejemplos de responsabilidad proactiva son el análisis del riesgo, la creación de un registro de actividades de tratamiento, la protección de datos desde el diseño y por defecto, la implementación de medidas de seguridad, la notificación de violaciones de seguridad de los datos, y en caso de que se observe un riesgo alto en el tratamiento de los datos personales, la evaluación de impacto sobre la protección de datos y el nombramiento de un DPD.

Análisis del riesgo.

Todos los responsables del tratamiento de datos deberán realizar un análisis del riesgo de los tratamientos que realicen, con el fin de establecer qué medidas deben aplicar y cómo hacerlo. El tipo de análisis variará en función de los tipos de tratamiento, la naturaleza de los datos, el número de interesados y la cantidad y variedad de tratamientos que la organización lleve a cabo.

En organizaciones de pequeño tamaño y con tratamientos de poca complejidad, la AEPD acepta que el análisis se base en "una reflexión, mínimamente documentada, sobre las implicaciones de los tratamientos en los derechos y libertades de los interesados." Esta reflexión deberá responder a cuestiones como:

- ¿Se tratan datos sensibles?
- ¿Se incluyen datos de una gran cantidad de personas?
- ¿Incluye el tratamiento la elaboración de perfiles?
- ¿Se cruzan los datos obtenidos de los interesados con otros disponibles en otras fuentes?
- ¿Se pretende utilizar los datos obtenidos para una finalidad para otro tipo de finalidades?
- ¿Se están tratando grandes cantidades de datos, incluido con técnicas de análisis masivo tipo "big data"?
- ¿Se utilizan tecnologías especialmente invasivas para la privacidad, como las relativas a geolocalización, videovigilancia a gran escala o ciertas aplicaciones del Internet de las cosas?

A mayor número de respuestas afirmativas, mayor es el riesgo y por tanto la necesidad de implementar mayores medidas de seguridad. Si la respuesta a estas preguntas fuera negativa, podemos concluir que el tratamiento de datos que realiza la organización no genera un riesgo elevado y no debe poner en marcha las medidas propuestas para este caso.

La AEPD pone a disposición de las PYMES la herramienta Facilita, que permite valorar a través de un cuestionario online la adecuación de la organización al RGPD y obtener los documentos mínimos indispensables para ayudar a cumplir con el Reglamento. Se recomienda la utilización de Facilita a aquellas empresas que realizan tratamientos de datos personales que, a priori, implican un escaso nivel de riesgo para los derechos y libertades de los interesados.

La AEPD presentó el 28 de febrero de 2018 su Guía Práctica de Análisis de Riesgos, para las organizaciones que no puedan utilizar su herramienta Facilita y deban llevar a cabo una evaluación del riesgo. La guía recoge metodología para realizar esta evaluación y plantillas y anexos de gran utilidad. Por otro lado, el Centro Criptológico Nacional pone a disposición de las PYMES la herramienta EAR/PILAR.

Registro de actividades de tratamiento.

Los responsables y encargados del tratamiento de datos deberán mantener un registro de operaciones de tratamiento en el que se recoja toda la información establecida en el RGPD. Éste deberá contener en todo caso:

- Nombre y datos del responsable del tratamiento de datos y del Delegado de Protección de Datos y existiese.
- Finalidades del tratamiento.
- Descripción de las categorías de interesados y categorías de datos personales tratados.
- Descripción de las categorías de destinatarios a quienes se comunican los datos personales.
- Transferencias internacionales de datos.
- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.
- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

Para organizar el registro de actividades de tratamiento, el responsable podrá partir de los ficheros que actualmente tiene notificados en el Registro General de Protección de Datos; en torno a operaciones que se realizan sobre cada conjunto estructurado de datos; o en torno a operaciones de tratamiento concretas vinculadas a una finalidad básica común de todas ellas (por ejemplo: gestión de clientes, gestión contable, gestión de nóminas, etc.).

Estarán exentas de mantener este registro aquellas organizaciones que empleen a menos de 250 trabajadores, a menos que el tratamiento que realicen pueda suponer riesgo para los derechos y libertades de los interesados; no sea ocasional; o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales.

La AEPD proporciona, en su nueva Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales Sujetos al RGPD, un modelo de registro de actividades de tratamiento que se puede tomar como base para la implantación de la medida en una organización.

Para facilitar la creación del registro de actividades de tratamiento, la AEPD ha facilitado la descarga del contenido de la inscripción en sus ficheros a través de este link.

Protección de datos desde el diseño y por defecto.

El RGPD recoge la necesidad de que, desde el inicio y durante el tratamiento, los responsables tomen medidas organizativas y técnicas para integrar en los tratamientos de datos las garantías que permitan aplicar de forma efectiva los principios contenidos en el texto legal. Además, deben adoptar medidas que garanticen que solo se traten los datos necesarios en lo relativo a la cantidad de datos tratados, la extensión del tratamiento, los periodos de conservación y la accesibilidad a los datos.

El artículo 32 del RGPD recoge, de forma no exhaustiva, algunas medidas que podrán ser aplicadas para garantizar un nivel de seguridad adecuado al riesgo. Ejemplos de estas medidas serían la seudonimización, que veremos más adelante, el cifrado de datos personales o la capacidad de restaurar la disponibilidad del acceso a los datos personales. El RGPD también establece una serie de principios relativos al tratamiento de datos que serán necesarios considerar cuando se diseñe un tratamiento:

- Licitud, lealtad y transparencia.
- Limitación de la finalidad.
- Minimización de datos.
- Exactitud.
- Limitación del plazo de conservación.
- Integridad y confidencialidad.

En resumen, lo que se intenta es que se piense en términos de protección de datos desde el momento en el que se diseña un tratamiento, un producto o un servicio que conlleve el manejo de datos personales, y garantizar así los derechos y libertades de los interesados.

Medidas de seguridad

A diferencia de la actual legislación, que determina con gran detalle y de forma exhaustiva las medidas de seguridad a aplicar según el tipo de datos tratados, el RGPD deja a juicio de los responsables y encargados del tratamiento de datos el establecimiento de las medidas técnicas y organizativas necesarias para garantizar un nivel de seguridad adecuado en función de los riesgos identificados en una evaluación previa. Para ello, el RGPD amplia las variables que deberán ser tomadas en cuenta:

- El coste de la técnica.
- Los costes de aplicación.
- La naturaleza, el alcance, el contexto y los fines del tratamiento.
- Los riesgos para los derechos y libertades.

El esquema de medidas de seguridad previsto en el Reglamento de Desarrollo de la LOPD no seguirá siendo válido automáticamente tras la fecha de aplicación del RGPD. En cualquier caso, los responsables podrán seguir aplicando las mismas medidas de seguridad si los resultados del análisis de riesgos concluyen que éstas son las más adecuadas para ofrecer un nivel de seguridad óptimo; o podrán utilizar las enumeradas en el Reglamento de Desarrollo de la LOPD como guía en el caso de necesitar implantar algunas nuevas.

La LOPDGGD ha optado por no introducir una nueva lista de medidas de seguridad a implantar por las empresas, aunque si llama a la Administración Pública a adoptar las medidas del Esquema de Seguridad Nacional. Habrá que estar a la espera de si la LOPDGGD es desarrollada, en este campo, mediante norma reglamentaria como se hizo con la anterior ley de protección de datos.

Notificación de violaciones de seguridad de los datos.

El RGPD define la violación de la seguridad de los datos personales como "toda violación de la seguridad que 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." Esta definición tan amplia, también llamada "quiebra de seguridad", incluye sucesos como la pérdida de un ordenador portátil o un móvil, el borrado accidental de ciertos ficheros e incluso el acceso no autorizado a bases de datos (incluso por el propio personal de la organización).

Cuando una violación se produzca, el responsable deberá comunicarla a la autoridad de protección de datos competente. La notificación deberá realizarse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella; y deberá incluir como mínimo:

- La naturaleza de la violación.
- Las categorías de datos y de interesados afectados.
- Las medidas adoptadas para solventar la situación.
- Las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados.

Se excluyen de la obligatoriedad de notificar los casos en los que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados, aunque si se establece la necesidad de registrar todas las violaciones de seguridad.

En los casos en los que tras la valoración del riesgo de la violación se concluya que ésta entraña un riesgo alto para los derechos y libertades de los interesados, se deberá notificar a éstos también para que puedan tomar las medidas oportunas para protegerse de sus consecuencias. Con esta finalidad en mente, el RGPD contempla la necesidad de que en la notificación a los interesados, en caso de violación de la seguridad, se incluyan propuestas de medidas a tomar por su parte.

La notificación a los interesados no será necesaria cuando:

- El responsable hubiera tomado medidas técnicas u organizativas apropiadas con anterioridad a la violación de seguridad, en particular las medidas que hagan ininteligibles los datos para terceros (cifrado, seudonimización o anonimización, por ejemplo). Se recomienda tomar medidas de esta naturaleza para evitar así el requerimiento legal de información a los usuarios, preservando la confianza de los interesados en la organización y su reputación.
- Cuando el responsable haya tomado con posterioridad a la quiebra medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice.
- Cuando la notificación suponga un esfuerzo desproporcionado, debiendo en estos casos sustituirse por medidas alternativas (una comunicación pública, por ejemplo).

La AEPD adaptará el canal específico para la notificación de las quiebras de seguridad en el ámbito de las comunicaciones electrónicas existente para poder ser utilizado en el marco del RGPD.

El Grupo del Artículo 29 preparará un formulario estandarizado a nivel supranacional para que esas notificaciones se realicen de forma armonizada a en toda la Unión Europea, garantizando que los responsables presentan unas notificaciones completas de acuerdo con los criterios del RGPD.

Seudonimización: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

La anonimización, por el contrario, no permitiría en ningún caso identificar a la persona a través de los datos. La AEPD cuenta con una sobre las orientaciones y garantías en los procesos de anonimización de datos que se puede consultar en el siguiente link: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Orientaciones_y_garantias_Anonimizacion.pdf

Evaluación de impacto sobre la protección de datos.

Cuando se determine que el tratamiento de datos conlleva un alto riesgo para los derechos y libertades de los interesados, los responsables de tratamiento deberán realizar una Evaluación de Impacto sobre la Protección de Datos, EIPD o PIA (por sus siglas en inglés, Privacy Impact Assessment), antes de iniciar el tratamiento.

Para determinar si es necesario llevar a cabo la EIPD, se puede seguir un análisis en dos fases: 1. Análisis de las listas de tratamientos previstos en el artículo 35 del RGPD; 2. Análisis de la naturaleza, alcance, contexto y fines del tratamiento. La regulación indica que hay que realizar una EIPD cuando un tratamiento puede suponer un alto riesgo para los derechos y las libertades de las personas físicas, especialmente si se utilizan nuevas tecnologías y teniendo en cuenta la naturaleza, alcance, contexto y finalidades del tratamiento.

Se considera en todo caso que los tratamientos conllevan un alto riesgo cuando éstos consistan en:

- Elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos sobre los interesados, o que les afecten significativamente de modo similar.
- Los tratamientos a gran escala de datos sensibles. La valoración del tratamiento a gran escala se realizará teniendo en cuenta: el número de interesados afectados; el volumen de datos y la variedad de datos tratados; la duración o permanencia de la actividad de tratamiento; y la extensión geográfica de la actividad de tratamiento.
- La observación sistemática a gran escala de una zona de acceso público (videovigilancia).

El RGPD recoge que la EIPD deberá contener como mínimo:

- Una descripción sistemática de las operaciones de tratamiento previstas y de sus fines.
- Una evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.
- Una evaluación de los riesgos para los derechos y libertades de los interesados.
- Las medidas previstas para afrontar los riesgos.

En el caso de que la EIPD se concluya con un riesgo residual elevado, el responsable del tratamiento deberá activar el procedimiento de Consulta Previa a la Autoridad de Control local y en ninguna circunstancia proceder a llevar a cabo el tratamiento objeto de evaluación.

La AEPD publicó el 28 de febrero de 2018 una nueva Guía de Evaluación de Impacto en la Protección de Datos para ayudar a las organizaciones a identificar las actividades que conllevan un alto riesgo y a establecer las medidas de control más adecuadas para minimizar el mismo antes de iniciar el tratamiento.

Las autoridades de protección de datos están obligadas a confeccionar listas adicionales de tratamientos que requieren una EIPD, y podrán también confeccionar listas de tratamientos que no requieran de EIPD.

Delegado de Protección de Datos (DPD).

El RGPD introduce la figura del Delegado de Protección de Datos (DPD), que será obligatoria en:

- Autoridades y organismos públicos.
- Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala.
- Responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles.

El nombramiento del DPD deberá ser realizado atendiendo a "sus cualificaciones profesionales, y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a sus capacidades" para desempeñar las funciones del puesto. La designación del DPD y sus datos de contacto deberá ser comunicada a la autoridad de supervisión competente y deberán ser hechos públicos por los responsables y encargados.

La AEPD ha optado por promover un sistema de certificación de profesionales de protección de datos para facilitar la evaluación de las cualificaciones profesionales y los conocimientos requeridos de los candidatos al puesto. En cualquier caso, la certificación no será un requisito indispensable para el acceso a la profesión.

ANF AC es la primera entidad de certificación en obtener la designación tras superar favorablemente la revisión efectuada por la Entidad Nacional de Acreditación.

El DPD deberá desarrollar sus funciones con los siguientes requisitos según el RGPD:

- Total autonomía en el ejercicio de sus funciones.
- Necesidad de que se relacione con el nivel superior de la dirección
- El responsable o el encargado deberá facilitar al DPD todos los recursos necesarios para desarrollar su actividad.

Se permite nombrar a un único DPD para un grupo de empresas siempre que sea accesible desde cada establecimiento del grupo. Del mismo modo, se permite que el DPD mantenga con responsables y encargados una relación laboral o mediante un contrato de servicios, y a tiempo completo o parcial, propiciando que el DPD sea una persona física u organización ajena al responsable o encargado.

La nueva LOPDGGD introduce en su artículo 34 una lista de entidades que deberán contar con la figura del DPD en todo caso. Entre éstas, encontramos colegios profesionales, centros docentes, entidades aseguradoras, entidades financieras, empresas de publicidad, y centros sanitarios, entre otros; y llama a la designación voluntaria en el resto de los casos.

Por otro lado, la LOPDGGD instaura la figura del DPD como intermediario entre el responsable del tratamiento de datos o el encargado y la AEPD y otras autoridades autonómicas de protección de datos, ya sea en comunicaciones entre las partes como en procesos sancionadores.

Capítulo 8. Transferencias internacionales.

Transferencias internacionales.

Los datos solo podrán ser comunicados fuera del Espacio Económico Europeo (países de la Unión Europea, Islandia, Liechtenstein y Noruega):

- A países, territorios, organizaciones internacionales y sectores específicos sobre los que la Comisión haya adoptado una decisión reconociendo que ofrecen un nivel de protección adecuado.
- Cuando se hayan ofrecido garantías adecuadas sobre la protección que los datos recibirán en su destino.
- Cuando se aplique alguna de las excepciones que permiten transferir los datos sin garantías de protección adecuada por razones de necesidad vinculadas al propio interés del titular de los datos o a intereses generales.

Las decisiones de adecuación y las cláusulas tipo para contrato adoptadas por la Comisión Europea con anterioridad a la entrada en vigor del RGPD seguirán siendo válidas hasta su derogación o sustitución por la misma. Las autorizaciones de transferencias otorgadas por las autoridades nacionales de protección de datos seguirán siendo válidas en tanto las autoridades no las revoquen.

El RGPD amplía la lista de instrumentos para ofrecer garantías, entre las que ahora se incluyen las normas corporativas vinculantes, cláusulas contractuales estándar, códigos de conducta y esquemas de certificación. En estos casos, la transferencia no requerirá la autorización de las autoridades de supervisión.

Normas corporativas vinculantes: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta.

Capítulo 9. Sanciones.

Sanciones

Competencia desleal

Sanciones.

El RGPD introduce el derecho de que todo interesado presente una reclamación ante una autoridad de control si considera que el tratamiento de sus datos personales, o de datos personales que le conciernen, infringe la normativa europea; y prevé multas mucho mayores que la actual normativa de protección de datos.

Frente a la cantidad máxima de 601.012,1 € prevista en la antigua LOPD, la autoridad de control podrá imponer sanciones a los responsables de tratamiento con los siguientes límites:

- 10.000.000 € como máximo o, si se trata de una empresa, hasta el 2% del volumen de negocio total anual del ejercicio financiero anterior.
- 20.000.000 € como máximo o, si se trata de una empresa, hasta el 4% del volumen de negocio total anual global del ejercicio financiero anterior.

Se optará siempre por la sanción de mayor cuantía.

Cabe también destacar el cambio en la naturaleza de los hechos sancionables. Con la anterior LOPD en mano, las sanciones se orientan a castigar la inacción del responsable en el tratamiento de datos o la obtención ilícita (o falta de) consentimiento del interesado; mientras que la RGPD y la nueva LOPDGDD centran las sanciones en casos de vulneración de los derechos de los interesados y el tratamiento inadecuado de los datos personales.

Por último, el RGPD deja margen a los Estados miembros para la determinación de los plazos de prescripción de infracciones y sanciones, y la determinación del régimen sancionador aplicable a las Administraciones Públicas, lo que España ha hecho con la publicación de la LOPDGGD.

La LOPDGGD sigue el modelo implantado desde Europa y divide las infracciones en muy graves, graves y leve, según el grado en que afecten a los datos. Así, entre las muy graves están aquellas acciones que supongan una vulneración sustancial del tratamiento, el uso de los datos para una finalidad distinta a la anunciada, la exigencia de pago para el acceso a los datos, etc., hasta un total de 17 casos; graves serán la obtención de datos de un menor sin el consentimiento debido, la falta de adopción de medidas técnicas adecuadas, la contratación de un encargado del tratamiento que no ofrezca las garantías necesarias, etc.; y como leves se contemplan todas aquellas que no se recojan en los dos grupos anteriores, como no informar, el incumplimiento de ciertas obligaciones por parte del encargado, etc. La LOPDGGD mantiene las cantidades máximas del RGPD.

En cuanto a la prescripción de estas sanciones, las muy graves prescribirán a los tres años; las graves a los 2 años; y las leves al año.

Competencia desleal.

Especial mención merece la Disposición adicional decimosexta de la LOPDGGD, que, en resumidas cuentas, considera prácticas agresivas a tenor de lo dispuesto en la Ley 3/1991, de 10 de enero, de Competencia Desleal, las siguientes:

- Realizar comunicaciones a responsables o encargados del tratamiento o a los interesados suplantando la identidad de la AEPD o una autoridad autonómica de protección de datos.
- Realizar comunicaciones simulando que se está actuando en nombre, por cuenta o colaboración con la AEPD u homólogo a nivel autonómico.
- Realizar prácticas comerciales en las que se coarte el poder de decisión de los interesados al hacer referencia a posibles sanciones por incumplimiento de la normativa de protección de datos.
- Ofrecer las llamadas “adaptación a coste cero”, es decir, ofrecer un documento por el que se pretenda crear una apariencia de cumplimiento de la normativa de protección de datos de forma complementaria a la realización de acciones formativas sin que se lleven a cabo las actuaciones necesarias para verificar que el cumplimiento se produce de forma efectiva.
- Asumir, sin designación debida, la función del DPD y comunicarse en tal condición con las autoridades de protección de datos.

El objetivo principal es perseguir y penar las prácticas desleales surgidas a raíz de la necesidad de adaptación de las empresas a las nuevas normas de protección de datos, que pueden ser víctimas de asesoramiento ineficaz o de ínfima calidad y que provoca su indefensión ante posibles sanciones o violaciones de la seguridad de los datos.

Capítulo 10. ¿Qué hacer para adaptarse a la nueva normativa de protección de datos?

¿Qué hacer para adaptarse a la nueva normativa de protección de datos?

¿Qué actuaciones deben emprender los responsables y los encargados del tratamiento para adecuar su actividad a la nueva regulación?

a) **Documentar las actividades de tratamiento**, mediante el mantenimiento de un registro de actividades de tratamiento que se lleven a cabo. Si la organización cuenta con ficheros notificados al Registro General de Datos, puede organizarlo relacionando los tratamientos con las finalidades con que notificó los ficheros. En éste se deberán anotar también las que se inicien una vez entre en vigor el RGPD.

b) **Evaluar e implantar las medidas de seguridad**, con el objetivo de determinar las medidas de seguridad que, de acuerdo con la nueva normativa, se deban implantar antes de la obligatoria aplicación del RGPD. Estas medidas deberán adaptarse a las características de los tratamientos, al tipo de datos tratados y la tecnología disponible en cada momento, pero en el caso de tratamientos que implican un riesgo bajo para los derechos y libertades de los interesados, no se requerirán medidas de seguridad más complejas que las contempladas como nivel básico en la legislación nacional vigente, por ejemplo.

c) **Establecer un protocolo para la notificación de las violaciones de seguridad**, tanto para la autoridad de protección de datos como para las personas afectadas.

d) **Revisar los mecanismos de recogida del consentimiento y la base jurídica del tratamiento**, especialmente cuando el consentimiento es la base jurídica del tratamiento que se lleva a cabo. Entre otros aspectos, hay que revisar que la recogida del consentimiento no se realice mediante casillas premarcadas o de forma tácita.

e) **Establecer mecanismos para facilitar el ejercicio de derechos y respuesta a las solicitudes de los interesados**, informando del modo de ejercer estos derechos. Estos mecanismos deberán ser diseñados por los responsables del tratamiento, pero pueden ser tan simples como proporcionar una dirección de email específica e identificar a un responsable de tramitar estas solicitudes.

f) **Revisar las cláusulas informativas**, atendiendo a los nuevos requisitos de transparencia y completando la información ofrecida en aquellos casos en los que la información se recogió con anterioridad a la entrada en vigor del RGPD.

g) **Revisar las cláusulas de los encargados de tratamiento**, incluyendo los nuevos requisitos en los contratos a firmar con posterioridad al 25 de mayo de 2018 y adaptando aquellos ya firmados. Ante todo, se deberán asegurar que los encargos de tratamiento de datos estén siempre amparados en un contrato de encargo con contenido distinto del que regula el servicio que se contrata.

h) **Revisar los mecanismos utilizados para transferir datos a terceros países**, verificando que se adecúan a la nueva regulación.

i) **Formar al personal** que intervenga en el tratamiento de datos de carácter personal y, en especial, a las personas que tengan atribuidas responsabilidades en esta materia dentro de la organización.

j) **Hacer la evaluación de impacto relativa a la protección de datos**, siempre que el tratamiento que se esté llevando a cabo suponga un riesgo alto para los derechos y libertades de las personas físicas y que permita la adopción de medidas correctoras de este riesgo.

k) **Hacer una consulta previa a la Autoridad de Protección de Datos**, siempre que de la evaluación de impacto sobre la protección de datos resulte que el tratamiento conllevaría un riesgo alto que no se haya mitigado.

l) **Designar un delegado de protección de datos**, si fuera necesario.

Capítulo 11. Lista de verificación.[1]

Legitimación

Información y derechos

Relaciones responsable-encargado

Medidas de responsabilidad proactiva

[1] Fuente: AEPD. *"Guía del Reglamento General de Protección de Datos para responsables del tratamiento".*

Legitimación

- ¿Tiene establecida claramente cuál es la base legal de los tratamientos que realiza y ha documentado de alguna forma el modo en que la ha establecido?
- Si alguno de los tratamientos que realiza está basado en el consentimiento de los interesados, ¿ha verificado que ese consentimiento reúne los requisitos que exige el RGDP? En caso contrario, ¿ha previsto cómo recabar el consentimiento de forma adaptada al RGPD o ha encontrado otra base legal adecuada para esos tratamientos?

Información y derechos.

- ❑ La información que se proporciona a los interesados, ¿está presentada de forma clara, concisa, transparente y de fácil acceso?
- ❑ ¿Contiene esa información todos los elementos que prevé el RGPD?
- ❑ ¿Dispone de mecanismos para el ejercicio de derechos visibles, accesibles y sencillos? ¿Pueden ejercerse los derechos por vía electrónica?
- ❑ ¿Tiene establecidos procedimientos o mecanismos que le permitan verificar la identidad de quienes solicitan acceso o ejercen los demás derechos ARCO?
- ❑ ¿Tiene establecidos procedimientos que le permitan responder a los ejercicios de derechos en los plazos previstos por el RGPD? ¿Ha valorado si sería necesaria la colaboración de los encargados para responder a las solicitudes de los interesados y, si es así, tiene previsto incluir esta colaboración en los contratos de encargo?
- ❑ En particular, ¿tiene previstos mecanismos para atender a posibles ejercicios del derecho a la limitación del tratamiento, de forma que los datos afectados puedan ser conservados sin ser objeto de las operaciones de tratamiento que corresponderían?
- ❑ ¿Ha valorado si los tratamientos de datos que realiza pueden ser objeto del derecho a la portabilidad? En caso, afirmativo, ¿ha previsto procedimientos o mecanismos para poder atender a este derecho y proporcionar los datos al interesado (o a otro responsable) en un formato estructurado, de uso común y susceptible de lectura mecánica?

Relaciones responsable-encargado.

- ¿Ha previsto cómo valorar si los encargados con los que haya contratado o vaya a contratar operaciones de tratamiento ofrecen garantías de cumplimiento del RGPD cuando sea de aplicación?
- ¿Contienen los contratos de encargo que actualmente tenga suscritos todos los elementos que prevé el RGPD? En caso contrario, ¿está dando pasos para adaptarlos antes de la aplicación del RGPD?

Medidas de responsabilidad proactiva.

- ❑ ¿Ha hecho una valoración de los riesgos que los tratamientos que desarrolla implican para los derechos y libertades de los ciudadanos? ¿Ha determinado qué medidas de responsabilidad activa corresponden a su situación de riesgo y cómo debe aplicarlas?
- ❑ ¿Ha previsto cómo establecer el registro de actividades de tratamiento en su organización?
- ❑ ¿Ha valorado si le es de aplicación alguna de las excepciones a esta obligación? ¿Ha previsto quién se encargará de mantener actualizado el registro?
- ❑ ¿Ha revisado las medidas de seguridad que aplica a sus tratamientos a la luz de los resultados del análisis de riesgo de los mismos? ¿Considera que puede seguir aplicando las medidas de seguridad previstas en el Reglamento de la LOPD? ¿Ha valorado suficientemente la posibilidad de introducir medidas adicionales en función del tipo de tratamiento o del contexto en que se realiza?
- ❑ Atendiendo al tipo de tratamientos que realiza, ¿ha establecido mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos?
- ❑ ¿Tiene previstas medidas de reacción frente a los diferentes tipos de quiebras de seguridad, incluidos los procedimientos para evaluar el riesgo que puedan suponer para los derechos y libertades de los afectados? ¿Ha establecido procedimientos para notificar las violaciones de seguridad a las autoridades de protección de datos y, si fuera necesario, a los interesados?
- ❑ ¿Dispone de un registro o herramienta similar en que pueda documentar los incidentes de seguridad que se produzcan, aunque no sean notificados a las autoridades de protección de datos?
- ❑ ¿Ha valorado si los tratamientos que realiza requieren una Evaluación de Impacto sobre la Protección de Datos porque supongan un alto riesgo para los derechos y libertades de los interesados?
- ❑ ¿Dispone de una metodología para la realización de la Evaluación de Impacto?
- ❑ Según el tipo de tratamiento que realiza y los resultados del análisis de riesgos previo, ¿tiene que nombrar un Delegado de Protección de Datos?
- ❑ ¿Ha establecido los criterios para seleccionar al Delegado de Protección de Datos y, en particular, para valorar sus cualificaciones profesionales y sus conocimientos?
- ❑ El puesto de DPD tal y como está configurado en su organización, ¿respeta los requisitos de independencia en el ejercicio de las funciones, posición en el organigrama, ausencia de conflicto de intereses y disponibilidad de los recursos necesarios establecidos por el RGPD?
- ❑ ¿Ha hecho pública la designación del DPD y sus datos de contacto y los ha comunicado a la autoridad de protección de datos?
- ❑ ¿Ha establecido procedimientos para que los interesados contacten con el DPD?

Bibliografía y otras fuentes de información.

Agencia Española de Protección de Datos (AEPD). Accesible online:

https://www.aepd.es/

AEPD. "*9ª Sesión Anual Abierta de la Agencia Española de Protección de Datos: preguntas de los asistentes*". Accesible online:

https://www.aepd.es/agencia/transparencia/jornadas/common/9-sesion/06-Preguntas-conjuntas-ponentes.pdf

AEPD. *"Adaptación al RGPD – Sector privado".* Accesible online:

https://www.aepd.es/media/infografias/infografia-adaptacion-rgpd-sector-privado.pdf

AEPD. *"Directrices para la elaboración de contratos entre responsables y encargados del tratamiento".* Accesible online:

https://www.aepd.es/media/guias/guia-directrices-contratos.pdf

AEPD. "*Guía del Reglamento General de Protección de Datos para responsables de tratamiento".* Accesible online:

https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

AEPD. "*Guía para el cumplimiento del deber de informar".* Accesible online:

https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf

AEPD. *"Guía para la gestión y notificación de brechas de seguridad".* Accesible online:

https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf

AEPD. "*Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD".* Accesible online:

https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

AEPD. "*Guía práctica para las evaluaciones de impacto en la protección de los datos sujetos al RGPD".* Accesible online:

https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

AEPD. "*Guía sobre el uso de videocámaras para seguridad y otras finalidades".* Accesible online:

https://www.aepd.es/media/guias/guia-videovigilancia.pdf

AEPD. "*Listado de cumplimiento normativo".* Accesible online:

https://www.aepd.es/media/guias/guia-listado-de-cumplimiento-del-rgpd.pdf

AEPD. "L*os derechos que tienes para proteger tus datos personales".* Accesible online:

https://www.aepd.es/media/infografias/infografia-rgpd-derechos-ciudadanos-aepd.pdf

AEPD. "*Novedades para el sector privado".* Accesible online:

https://www.aepd.es/media/docs/novedades-lopd-sector-privado.pdf

AEPD. "*Novedades para los ciudadanos".* Accesible online:

https://www.aepd.es/media/docs/novedades-lopd-ciudadanos.pdf

AEPD. "*Protección de Datos: Guía para el Ciudadano".* Accesible online:

https://www.aepd.es/media/guias/guia-ciudadano.pdf

AEPD. "*Orientaciones y garantías en los procedimientos de anonimización de datos personales".* Accesible online:

https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

AEPD y CEPYME. "*Encuesta sobre el grado de preparación de las empresas españolas ante el reglamento general de protección de datos*". Accesible online:

https://www.aepd.es/media/estudios/estudio-proteccion-de-datos-aepd-cepyme.pdf

Agencia Estatal Boletín Oficial del Estado (BOE). Accesible online:

https://www.boe.es/diario_boe/

Agencia Vasca de Protección de Datos. Accesible online:

http://www.avpd.euskadi.eus/s04-5213/es/

Autoridad Catalana de Protección de Datos (ACPD). Accesible online:

http://apdcat.gencat.cat/es/inici/

ACPD. "*Guía para el cumplimiento del deber de informar en el RGPD".* Accesible online:

http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/V10-ES-Guia-sobre-el-deber-de-informar-en-el-RGPD-con-diseno.pdf

ACPD. "*Guía sobre la evaluación de impacto relativa a la protección de datos en el RGPD (2.0)".* Accesible online

http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/GUIA-EVALUACION-DE-IMPACTO-CAST-2.0.pdf

Comisión Europea. *"¿Cómo reforzará la reforma de la protección de datos en la UE el mercado interior?".* 2016. Accesible online:

http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41591

Comisión Europea. *"¿Cómo refuerza la reforma de la protección de datos los derechos de los ciudadanos?".* 2016. Accesible online:

http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41596

Comisión Europea. *"Mejores normas para las empresas europeas".* 2018. Accesible online:

https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-business_es.pdf

Comisión Europea. *"Reforma de la protección de datos en la UE: Ventajas para las empresas en Europa".* 2016. Accesible online:

http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41595

Comisión Europea. *"Siete pasos para que las empresas se preparen para el Reglamento general de protección de datos (RGPD)".* 2018. Accesible online:

https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-es-n_0.pdf

Confederación de Consumidores y Usuarios. "*Guía práctica para la protección de los datos e información de carácter personal*". Accesible online:

http://cecu.es/campanas/cuadernos/LOPD_1.pdf

Grupo de Trabajo del artículo 29. Accesible online:

https://ec.europa.eu/newsroom/article29/news-overview.cfm

Grupo de Trabajo del artículo 29. "*Directrices sobre los delegados de protección de datos (DPD)*". Accesible online:

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

Grupo de Trabajo del artículo 29. "*Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*". Accesible online:

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051