Interreg
España - Portugal
Espacio Talento Joven
Fondo Europeo de Desarrollo Regional

ildefe
AYUNTAMIENTO DE LEÓN

RGPD

Reglamento General de protección de Datos

LO QUE HAY QUE TENER EN CUENTA

Manual para emprendedores y micropymes

Esta publicación se edita en el marco de los trabajos del proyecto **ESPACIO TALENTO JOVEN**, cofinanciado por el Fondo Europeo de Desarrollo Regional (FEDER) a través del Programa Interreg V-A España-Portugal (POCTEP) 2014-2020

Eje prioritario 2: Crecimiento integrador a través de una cooperación transfronteriza a favor de la competitividad

ÍNDICE DE CONTENIDOS

A. INTRODUCCIÓN

En mayo de 2016 se aprobó en el Parlamento Europeo el denominado **Reglamento General de Protección de Datos (RGPD)**, para todos los países miembros de la Unión Europea, y que sustituye a la conocida LOPD (Ley Orgánica de Protección de Datos de carácter Personal en España). Esta nueva normativa es aplicable y obligatoria dos años después: desde el **25 de mayo de 2018**, fecha en la que personas, empresas y entidades que traten o manejen datos personales deberán cumplir, para estar completamente adaptados a sus requisitos y exigencias.

El **RGPD** contiene novedades sustanciales, con el fin de afrontar los actuales retos, especialmente por el extenso uso de las nuevas tecnologías en todos los ámbitos de cada actividad empresarial.

Se incorporan los principios de **responsabilidad proactiva** y el **enfoque de riesgo**, además se incluye la obligación general (para todos los responsables) de realizar una valoración de ese riesgo, que será más o menos compleja según el tamaño de la organización y la cantidad de información a tratar.

Si bien el Reglamento es directamente aplicable y no requiere de trasposición posterior a la legislación nacional, en España existe ya un proyecto aprobado para esta nueva norma de "*Protección de Datos Personales*", que podría venir a puntualizar algunos aspectos.

El objeto de este documento, es proporcionar a emprendedores y pymes una orientación (aunque no de forma exhaustiva), sobre las **obligaciones** que conlleva el nuevo **Reglamento General de Protección de Datos (RGPD)**, destacando las principales diferencias respecto a la normativa que se venía aplicando en nuestro país (Ley orgánica de Protección de Datos Personales y su reglamento de desarrollo: LOPD).

B. DEFINICIONES Y ABREVIATURAS

- **Datos personales:** toda información concerniente a una persona física identificada o identificable, 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.

- **Tratamiento de datos:** 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.

- **Datos sensibles (art. 9 RGPD):** datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

- **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 (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.

- **Encargado de tratamiento (encargado):** la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

ABREVIATURAS EMPLEADAS EN ESTE MANUAL:

- **AEPD:** Agencia Española de Protección de Datos. En España, es la autoridad pública independiente encargada de velar por la privacidad y la protección de datos de los ciudadanos.
- **LOPD:** Ley Orgánica de Protección de Datos Personales (Ley 15/1999, de 13 de diciembre, de protección de datos de carácter personal y su reglamento de desarrollo RD 1720/2007).
- **RGPD:** Nuevo y actual Reglamento General de Protección de Datos (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 y por el que se deroga la Directiva 95/46/CE).
- **EIPD:** evaluación del impacto en la protección de datos.
- **DPD:** delegado de protección de datos.

C. RECOMENDACIÓN INICIAL

Análisis de nuestro punto de partida

Para empezar, se recomienda recoger información sobre los datos personales que tratamos actualmente en nuestra actividad. Sobre todo nos fijaremos en lo siguiente:

- De quién son los datos personales que tratamos en nuestra actividad (clientes, proveedores, trabajadores, etc.) En definitiva, quiénes son nuestros **interesados**, respecto a la protección de datos.

- Qué **datos personales** (y sólo personales) tratamos de cada interesado. Por ejemplo, respecto a los trabajadores: nombre, fechas de nacimiento, dirección, datos de formación…), imágenes de videovigilancia, etc.

- Los **fines** y los **tratamientos** de que son objeto cada grupo de datos, o sea, para qué los utilizamos y qué hacemos con ellos.

- Revisar si, en algún caso, tenemos **datos personales sensibles** según el nuevo Reglamento (por ejemplo, si prestamos un servicio sanitario y disponemos de datos de salud de nuestros pacientes) o si en algún caso afectan a **menores**.

- Revisar si hacemos **tratamientos masivos de datos**, o los utilizamos para la **elaboración de perfiles**, según la definición del Reglamento.

Casi todas las actividades comerciales van a disponer, como mínimo de datos personales de clientes y/o proveedores (de contacto, para facturar, etc.), de trabajadores (datos de contacto, datos por nóminas…), candidatos (solicitudes de empleo), pero también debemos tener en cuenta los datos de usuarios web (obtenidos, por ejemplo de formularios de solicitud de información), etc.

Nota: en el caso de que ya se cumpla con la normativa anterior (LOPD), esta información se puede obtener fácilmente de los ficheros que tendremos inscritos actualmente en la Agencia Española de Protección de Datos (AEPD), si bien es conveniente revisar que esté actualizada y completa respecto a todos los datos personales que manejamos y los tratamientos que realizamos.

D. OBLIGACIONES QUE AFECTAN A TODOS

1. Realizar un Análisis de Riesgos

Una de las principales novedades que incorpora el Reglamento, es la obligación de realizar inicialmente un **Análisis de Riesgos**, para determinar qué medidas de seguridad se deben aplicar a cada tratamiento de datos personales. Esto persigue que se planifique la "privacidad desde el diseño y por defecto", de forma que se incluyan las medidas adecuadas de privacidad desde el momento en que se está diseñando una determinada actividad que conlleve el tratamiento de datos.

De una forma u otra, debe quedar alguna evidencia de que se ha realizado este análisis y de que las conclusiones son coherentes, ya que la autoridad de control lo puede requerir en cualquier momento.

¿Cómo se realiza un análisis de riesgos? Dependerá de si, a priori, somos o no susceptibles de tener tratamientos de riesgo elevado. Habrá cierto riesgo en el tratamiento de datos personales, cuando:

- Se traten datos sensibles (ver la definición)
- Se disponga de datos de gran cantidad de personas
- Se elaboren perfiles
- Se crucen datos de los interesados con otros disponibles en diversas fuentes
- Se pretendan usar los datos para otras finalidades distintas para las que fueron obtenidos
- Se tratan gran cantidad de datos personales (incluido análisis masivo, big data)
- Se usan tecnologías especialmente invasivas par la privacidad (geolocalización, videovigilancia a gran escala, etc.)

En caso de que, a priori, **NO** se vayan a realizar estos tratamientos de riesgo, la AEPD ha desarrollado una herramienta en su web para cumplir el requisito (FACILITA RGPD), mediante un cuestionario sencillo. Si la herramienta concluye que, efectivamente, no se habrá tratamiento de riesgo, este cuestionario puede servir de evidencia de que hemos realizado el obligatorio análisis de riesgos.

En el caso de que la herramienta revele que sí podríamos ser susceptibles de tener tratamientos de alto riesgo, se debería realizar un análisis más en profundidad según las guías de la Agencia u otra metodología de análisis de riesgos valida.

2. Aplicar medidas de seguridad

El nuevo Reglamento ya no cuenta con la clasificación de riesgo bajo, medio o alto de la normativa anterior, y deja abierta la selección de medidas en función del análisis de riesgo inicial que realice cada responsable.

Si no se tienen tratamientos de riesgo elevado, el cuestionario de la AEPD puede servir de apoyo para implementar unas medidas de seguridad básicas, que se incluyen en el documento final que proporciona la herramienta FACILITA RGPD. En principio, las medidas de seguridad que se venían aplicando hasta ahora, podrían seguir siendo válidas, pero deben estar fundamentadas en un análisis de riesgos, en otros casos, habrá que modificarlas. Por poner varios ejemplos, estas medidas podrían ser:

- **Medidas organizativas:** acceso restringido a locales para terceros, archivo de documentos bajo llave, bloqueo de pantallas en caso de inactividad, destrucción de datos antes de desechar documentos, firma de acuerdos de confidencialidad con empleados…
- **Medidas técnicas:** acceso personalizado y con contraseña a sistemas de información, contraseñas seguras y cambio periódico de las mismas, copias de seguridad, antivirus y cortafuegos, cifrado de datos…

Habrá que tener en cuenta que las medidas de seguridad deben estar implantadas **antes de comenzar a tratar los datos.** Por lo tanto, se debería de pensar con suficiente antelación en las implicaciones que cada actividad conlleve en los datos personales, analizar el riesgo e incluir las medidas organizativas y técnicas necesarias, **siempre previamente a cualquier tratamiento de datos.**

El personal que acceda o trabaje con datos personales deberá estar debidamente formado sobre las medidas de seguridad que debe aplicar en cada caso, y en el procedimiento para atender los derechos de los interesados.

3. Permitir el ejercicio de sus derechos a los interesados

Los interesados de los que disponemos datos personales tienen los siguientes derechos:

- Acceder a sus datos personales (e incluso a obtener una copia)
- A que se rectifiquen sus datos si son erróneos o incompletos
- A que se supriman sus datos (derecho al olvido) en determinadas circunstancias
- A limitar el tratamiento de sus datos
- A ser informado sobre la rectificación, supresión o limitación del tratamiento de sus datos, salvo que ello exija un esfuerzo desproporcionado al responsable
- A la portabilidad de sus datos automatizados (siempre que sea técnicamente posible, por ejemplo, la transmisión de datos de un usuario del operador de telefonía en el que cursa baja del servicio, al nuevo operador en el que se da de alta)
- Oposición a que sus datos se usen para decisiones automatizadas y elaboración de perfiles

Se debe disponer, por tanto, de la sistemática necesaria para atender cualquier petición y de un canal de comunicación accesible para los interesados. También será imprescindible que nuestro personal esté formado para realizar este tipo de actuaciones.

4. Informar a los interesados

Paralelamente a las acciones anteriores, se debe facilitar determinada información a los interesados de quienes obtengamos datos personales. Lo más habitual es disponer de **cláusulas informativas** en los soportes, donde se recogen este tipo de datos (contratos, presupuestos, facturas, formularios para el personal, formularios web, etc.). Es necesario también contar con una **Política de Privacidad** en nuestra web que incluya esta información.

Según el nuevo RGPD, la información a incluir será la siguiente:

Identidad y datos de contacto del responsable del tratamiento	El plazo durante el cual se conservarán los datos, o los criterios para determinar ese plazo
Contacto del delegado de protección de datos, en caso de que haya que designarlo (ver más adelante)	El deber del interesado a ejercitar sus derechos (acceso, rectificación, supresión, limitación del tratamiento, oposición al mismo, así como a la portabilidad de los datos)
Fin del tratamiento y base jurídica	La existencia del derecho del interesado a retirar su consentimiento, cuanto el tratamiento se base en su persona

Intereses legítimos del responsable o un tercero (cuando el tratamiento se base en él)	El derecho a presentar una reclamación ante una autoridad de control
Destinatarios o categorías de destinatarios de los datos personales, en su caso	Si la comunicación de datos es un requisito legal o contractual
En su caso, la intención de transferencias de datos a un tercer país	La existencia de decisiones automatizadas, incluida la elaboración de perfiles

La información debe proporcionarse en el momento en que se obtengan los datos y ser concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular si está dirigida a niños. Se dará por escrito o por otros medios, inclusive si procede, por medios electrónicos.

Nota: si los datos no se obtuvieran directamente del interesado:

- Se debe informar, además de todo lo anterior, de la fuente de la que se han obtenido esos datos, antes de un mes desde que se obtuvieron, o en el momento de la primera comunicación con el interesado.
- No será necesario informar, cuando resulte imposible o un esfuerzo desproporcionado, cuando su obtención esté amparada por el derecho, o cuando los datos deban seguir teniendo carácter confidencial por un deber legal de secreto profesional.

Respecto a la **base jurídica**, podemos basarnos en el consentimiento del interesado, pero podrían aplicarse otras opciones como: que sea necesario para la ejecución de un contrato, para cumplir una obligación legal, para proteger intereses vitales, interés público o intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos (en éste último caso, siempre que no prevalezcan los intereses o los derechos y libertades fundamentales del interesado, en particular cuando sea un niño).

El siguiente ejemplo es un caso sencillo, en el que la empresa no estaría obligada a tener **DPD** (Delegado de Protección de Datos), pues no hay cesión de datos ni transferencias a terceros países, ni elaboración de perfiles:

En nombre de la EMPRESA xxxxxxxx, con CIF: B-xxxxxxx, dirección postal xxxxx, teléfono xxxxxx, correo electrónico xxxxx, le comunicamos que tratamos la información que nos facilita con el fin de prestarle el servicio solicitado y realizar la facturación del mismo. Los datos proporcionados se conservarán mientras se mantenga la relación comercial o durante los años necesarios para cumplir con las obligaciones legales. Estos datos no se cederán a terceros salvo en los casos en que exista una obligación legal para hacerlo. Tiene derecho a obtener

información para saber si en la EMPRESA xxxxxx se están tratando sus datos personales, por tanto tiene derecho al acceso, rectificación, limitación de tratamiento, supresión, portabilidad y oposición al tratamiento de sus datos de carácter personal.

Podrá dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna.

En otros casos, si fuera aplicable el resto de información, puede ser recomendable facilitarla en dos capas, por ejemplo, aportando los datos adicionales en el reverso de los documentos, en un anexo, expuesta al alcance de los interesados (y de la que se pueda obtener copia), o en una página web a la que se haga referencia en el documento principal, etc. Añadiendo, por ejemplo:

Puede consultar información adicional y detallada sobre Protección de Datos en nuestra página web: _____ (se facilitará el hipervínculo a la información y en ella se incluirían los datos aplicables, por ejemplo contacto del **DPD**, la intención de realizar transferencias internacionales, etc.)

La AEPD dispone de una guía exhaustiva para dar cumplimiento a esta obligación: "Guía para el cumplimiento del deber de informar".

5. Obtener el consentimiento de los interesados.

Cuando se necesite el consentimiento del interesado, este debe obtenerse de forma **inequívoca**. **¿Esto qué significa?:**

Consentimiento inequívoco *es aquel que se ha prestado mediante una manifestación del interesado o mediante una clara acción afirmativa.*

Esto implica que **NO** se admiten formas de consentimiento tácito o por omisión (por ejemplo, mediante la inclusión de cláusulas en la que le indicamos al interesado que, si no nos comunica nada en un determinado plazo, nos da su consentimiento), ni con casillas pre-marcadas.

El consentimiento inequívoco puede ser **implícito o explícito.**

Consentimiento inequívoco implícito: cuando se deduce de una acción del interesado (por ejemplo, cuando el seguir navegando en una web implica la aceptación del uso de cookies)

Consentimiento inequívoco explícito: cuando el interesado manifiesta explícitamente su consentimiento, por ejemplo, mediante la firma de un documento al efecto.

El consentimiento, ha de ser **inequívoco en todos los casos**, pero sólo ha de ser **explícito** cuando:

- Se traten datos sensibles (ver definiciones)
- Se adopten decisiones automatizadas
- En las transferencias internacionales de datos

Se deberá elaborar o revisar (si ya se cumple con la LOPD), las cláusulas o soportes en los que se recoge actualmente el consentimiento de los interesados, adaptándolos a este requisito.

Siguiendo con el ejemplo del apartado anterior, la empresa desea emplear los datos personales del cliente, además de para facturar y hacer pedidos, para ofertarle otros productos. A la cláusula informativa se le incluye lo siguiente, de lo cual deberemos guardar copia:

Solicito su autorización para ofrecerle productos y servicios relacionados con los solicitados y fidelizarle como cliente.

Si

No

Le informamos de que podrá revocar en cualquier momento el consentimiento prestado enviando un email a la dirección de correo indicada: xxxxxx.

Consentimiento de menores:

El consentimiento en el caso de menores, en el ámbito de la oferta directa de servicios de la sociedad de la información, será válido a partir de los 16 años (cada país podrá establecer otro límite, pero nunca inferior a 13 años (*). Por debajo de esa edad, se requiere la autorización de los padres o tutores legales, y se deben de efectuar esfuerzos razonables para verificar que el consentimiento fue dado o autorizado por la patria potestad o tutela del niño, teniendo en cuenta la tecnología disponible.

Nota (*): la normativa actual en España, contempla este límite con carácter general, en los 14 años. Habrá que ver si la próxima Ley nacional, que se encuentra en elaboración, modifica o no este límite de edad.

6. Establecer contratos con los encargados de tratamiento

Encargados de tratamiento: aquellas empresas o personas que tratan datos personales de nuestra responsabilidad, por ejemplo, la asesoría laboral que nos elabora las nóminas, la empresa informática que puede acceder a datos personales de nuestros clientes, servicios de almacenamiento en la nube, etc. También debemos tener en cuenta que nosotros podemos ser encargados de tratamiento respecto a otros responsables.

Las principales obligaciones de un encargado de tratamiento, son mantener un registro de las actividades de tratamiento, determinar las medidas de seguridad aplicables a los tratamientos que realizan y designar un **DPD** (en los casos en que sea aplicable).

Siguiendo el principio de responsabilidad activa, el responsable de tratamiento sólo debe contratar encargados de tratamiento que le puedan proporcionar suficientes garantías de que tratará los datos personales con seguridad. Aunque no es obligatorio, seleccionar encargados adheridos a Códigos de Conducta aprobados por la AEPD o certificaciones específicas en protección de datos, puede facilitarnos dicha obligación.

Debe formalizarse un **Contrato** con cada encargado del tratamiento, con los siguientes contenidos mínimos:

Objeto, duración, naturaleza y finalidad del tratamiento
Tipo de datos personales y categorías de interesados
Obligación del encargado de tratamiento de tratar los datos únicamente siguiendo instrucciones documentadas del responsable
Condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones
Asistencia al responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados

Por tanto, se debe identificar quiénes son nuestros encargados de tratamiento y establecer con ellos un Contrato que abarque, como mínimo, estos puntos.

Si ya cumplíamos con la LOPD anterior, revisaremos los contratos de encargo existentes, y los volveremos a formalizar con cada uno de los encargados. La AEPD también dispone de una guía exhaustiva sobre esta obligación.

7. Notificar las "Violaciones de Seguridad de los Datos"

Se conocen comúnmente como "quiebras de seguridad": por ejemplo, pérdidas de soportes con datos, accesos no autorizados a redes internas, etc.

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.*

1. Las violaciones de seguridad **deben documentarse siempre**. Se debe dejar registro interno de lo que pasó, las consecuencias y las medidas tomadas. En caso de inspección, nos podrían requerir este registro.

2. Además, deberán **notificarse a la AEPD**, a menos que sea improbable que suponga un riesgo para los derechos y libertades de los afectados. Requisitos de esta Notificación:

- Debe realizarse, a ser posible, dentro de las 72 horas siguientes a tener constancia de ella.
- Contenido mínimo de la comunicación:
  - Naturaleza
  - Categorías de datos e interesados afectados y número aproximado de afectados
  - Medidas adoptadas para solventarla y, si aplica, para paliar efectos negativos a los afectados
  - Contacto donde obtener más información

3. En el caso de violaciones de **Alto Riesgo** (por ejemplo: que se desvele información como contraseñas, participación en determinadas actividades, o difusión masiva de datos sensibles) debe acompañarse, además, de una **notificación dirigida a los afectados**.

Dicha notificación a los afectados podría no ser necesaria en caso de que se disponga de medidas que hagan ininteligibles los datos, por ejemplo, si se usa cifrado, o bien si se toman medidas posteriores que impidan el riesgo. Tampoco sería necesario en caso de que suponga un esfuerzo desproporcionado para el responsable o encargado.

E. OBLIGACIONES QUE PUEDEN SER APLICABLES O NO

1. Registrar las actividades de tratamiento

A diferencia de la normativa anterior, que exigía en todo caso dar de alta en la AEPD todos los ficheros de datos personales, están exentas de esta obligación las organizaciones con menos de 250 trabajadores, salvo que realicen tratamientos que puedan entrañar un riesgo para los derechos y libertades, no sea ocasional o incluya categorías especiales de datos o relativos a condenas e infracciones penales.

En el caso de que sí se nos aplique esta obligación, la página web de la AEPD ya permite obtener de forma automatizada esta información, a partir de los ficheros que tenga el responsable dados de alta con anterioridad. En cualquier caso, este registro debe ponerse a disposición de la autoridad de control si lo solicita.

2. Realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD)

Se exige su realización cuando sea probable que el tratamiento **«entrañe un alto riesgo para los derechos y libertades de las personas físicas»** (artículo 35, apartado 1). La EIPD es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales, en función de las actividades de tratamiento que se llevan a cabo con los mismos.

Se deberá realizar la EIPD, antes de comenzar a tratar datos o en el caso de que se tenga previsto hacer tratamientos con los siguientes tipos de datos

- Elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente
- Tratamiento a gran escala datos sensibles
- Observación sistemática a gran escala de una zona de acceso público
- Otros tratamientos que la autoridad nacional incluya en las listas adicionales que elabore
- Otros tratamientos que puedan conllevar un alto riesgo para los derechos y las libertades de los interesados, aunque no estén entre los anteriores

Hay alguna excepción en cuanto a la obligatoriedad de su realización, y a priori, tampoco es necesario realizarla si los tratamientos ya se venían efectuando antes de la

aplicación del Reglamento, pero en este caso, en el momento en que cambie cualquier circunstancia del tratamiento, habría que elaborar la EIPD.

No se exige una metodología concreta para efectuarla, pero sí existe una Guía en la web de la AEPD que puede servir de orientación para su realización e indica cuales son los criterios para su obligatoriedad.

Si, una vez realizada la evaluación, se identifica un alto riesgo que no pudiera ser mitigado por medios razonables, el responsable deberá realizar una **Consulta a la Agencia de Protección de Datos**. Esta autoridad podrá emitir recomendaciones o incluso prohibir el tratamiento.

3. Designar un Delegado de Protección de Datos (DPD)

Esta nueva figura que crea el Reglamento, es obligatorio designarla en determinados casos:

- Autoridades y administraciones públicas
- Operaciones de tratamiento con observación habitual y sistemática de interesados a gran escala
- Tratamiento a gran escala de datos sensibles

Sin embargo, el Reglamento no exige una titulación específica, pero el **DPD** (Delegado de Protección de Datos) sí debe poseer conocimientos especializados en derecho y en la práctica de la protección de datos.

NOTA: la AEPD ya ha puesto en marcha una certificación específica (pero no obligatoria) para las personas que quieran acreditar que reúnen las cualificaciones profesionales y conocimientos requeridos para ejercer esta profesión. Esto puede ser una garantía para los responsables que necesiten designar esta figura, a la hora de seleccionar al candidato/a más idóneo.

En caso de que esta obligación nos afecte, debemos hacer pública su designación, así como sus datos de contacto. La AEPD cuenta ya con un formulario web para cumplir con este requisito.

El **DPD** puede ser personal interno o externo a la organización. Debe tenerse especial cuidado, en el caso de que sea personal de la organización, con los conflictos de intereses, ya que el DPD ejerce funciones de supervisión, por lo que no debería revisar su propio trabajo. Por ejemplo, podría haber conflicto al designar al responsable TIC como DPD, si se emplean tecnologías de la información para tratar datos personales.

Además el DPD cuenta con funciones específicas, indicadas en el Reglamento, como son el asesoramiento al responsable en materia de protección de datos, la supervisión del cumplimiento, la cooperación con la autoridad de control y servir de contacto con la misma, entre otros.

4. Transferencias internacionales

Si realizamos cualquier operación con países de fuera de la UE que implique transferencia de datos personales a los mismos, sólo se podrán comunicar datos personales fuera del Espacio Económico Europeo:

- A países, territorios o sectores específicos (el RGPD incluye también organizaciones internacionales) 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. Como novedad, se incluye como garantía "adecuada", disponer de Normas Corporativas vinculantes, cláusulas contractuales estándar, códigos de conducta y esquemas de certificación.

- 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

- Por lo tanto, las decisiones y autorizaciones de la Comisión relativas a las transferencias internacionales, adoptadas con anterioridad al nuevo RGPD siguen siendo válidas hasta que la Comisión no las sustituya o derogue.

F. SANCIONES

Es destacable el **endurecimiento de las sanciones** que conlleva el nuevo Reglamento, tanto para los responsables como para los encargados del tratamiento de datos personales.

Se prevén multas de hasta 20 millones de euros o tratándose de una empresa, pueden conllevar una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Respecto a otras obligaciones, este límite baja hasta los 10 millones de euros o el 2%, cantidades relevantes, en cualquier caso.

A estas sanciones podría añadirse además, la posible indemnización a los interesados que hayan sufrido daños y perjuicios materiales o inmateriales por infracciones respecto a la protección de datos (artículo 82).

Avenida de la Magdalena 9, 24009 León

985 235 040

ildefe@ildefe.es

www.ildefe.es