# INFORME SOBRE EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

El 24 de mayo de 2016, entró en vigor el nuevo 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, o lo que es lo mismo el **REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS**, que pretendemos explicar y sintetizar en el siguiente informe a petición del **Consejo General de Colegios Oficiales de Podólogos de España.**



## ¿QUÉ ES EL RGPD? ¿CUÁNDO SERÁ DE OBLIGATORIO CUMPLIMIENTO? ¿QUIÉN DEBERÁ CUMPLIR CON ÉL?

Desde que entró en vigor en el año 2000 la **Ley Orgánica de Protección de Datos (LOPD)**, y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, Reglamento que la desarrolla, se les viene exigiendo a los responsables y a los encargados del tratamiento de datos de carácter personal, el cumplimiento de determinadas obligaciones en cuanto al tratamiento de datos se refiere.

La novedad en este ámbito se produjo, como bien sabemos, el 24 de mayo de 2016, fecha en la que entró en vigor el nuevo **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, o lo que es lo mismo el Reglamento General de Protección de Datos. El contenido regulado en este nuevo reglamento, supone una modificación sustancial del contenido de la vigente LOPD, exigiendo a las empresas nuevas obligaciones en materia de protección de datos y estableciendo durísimas sanciones a aquellas que no cumplan con el reglamento.

No obstante, a pesar de que el RGPD está en vigor desde abril de 2016, **no será de obligatorio cumplimiento hasta el 25 de mayo de 2018**. El legislador ha otorgado un periodo de dos años a las empresas para que vayan adoptando las medidas pertinentes para el efectivo cumplimiento del mismo.

Al tratarse de un Reglamento de la UE, no es necesaria la trasposición de su contenido al ordenamiento interno de cada EM, sino que es de **aplicación directa**. A pesar de su efecto directo y con ánimo de adaptarse al contenido del Reglamento, España es uno de los países más avanzados en materia legislativa ya que el 27 de junio de 2017 presento un anteproyecto de Ley de Protección de Datos.



En definitiva, toda empresa deberá de cumplir con el RGPD a partir del 25 de mayo de 2018, de lo contrario, se les podrá sancionar con importantes multas de hasta 20 millones de euros o incluso del 4% de su facturación.

Estarán obligadas al cumplimiento del RGPD todas las empresas que tengan algún establecimiento abierto en la Unión Europea y también aquellas que, sin tenerlo, presten servicios en el ámbito comunitario a residentes de la Unión Europea, con total independencia de dónde se produzca el tratamiento de los datos, de manera que **el Consejo General de Colegios Oficiales de Podólogos de España también debe cumplir con el mismo.**

## ¿QUÉ MEDIDAS DEBERÁN ADOPTAR EL CONSEJO GENERAL PARA CUMPLIR CON EL NUEVO RGPD?

El RGPD introduce nuevas medidas que deberán de ser adoptadas por el Consejo General de Colegios Oficiales de Podólogos de España. Una de los pilares sobre los que rige el RGPD es el denominado ***principio de Responsabilidad Activa***. La responsabilidad activa implica que las empresas deberán de prever los riesgos que el tratamiento de los datos pueda ocasionar, así como los daños que pueda generar, **no siendo suficiente con actuar una vez se ha producido el problema**.

Para cumplir con dicho principio, **el Consejo General de Colegios Oficiales de Podólogos de España deberá de adoptar una serie de medidas con el fin de garantizar la protección de los datos de sus clientes y/o asociados/miembros, y con la finalidad de prevenir riesgos y daños que puedan producirse en el tratamiento de los mismos**. Este nuevo reglamento refleja determinadas medidas cuya principal finalidad será la prevenir riesgos derivados del tratamiento de datos y la de garantizar la legalidad del tratamiento. Las medidas más importantes son:



- Proteger los datos desde el diseño y por defecto
- Establecer medidas de seguridad en función del riesgo del tratamiento
- Mantenimiento de un registro de tratamientos
- Realizar evaluaciones de impacto sobre la protección de datos
- Nombrar un delegado de protección de datos
- Notificar a la autoridad competente en un plazo de 72 horas de todas aquellas violaciones de la seguridad de los datos

Calle Barceló nº 1, 1º Izda. - 28004 - Madrid - Telf.: 91 532 00 09 - Fax: 91 522 78 94
hya@hebreroyasociados.com

- Promover y elaborar códigos de conducta y esquema de certificación que garanticen el cumplimiento de las obligaciones a las que el RGPD hace referencia.

## ¿QUÉ TÉRMINOS DEBO COMPRENDER PARA ENTENDER EL RGPD?

Antes de analizar los sujetos que componen la relación en materia de protección de datos, es importante esclarecer qué entiende la normativa por ***datos de carácter personal***. Para ello, hemos acudido al art. 3 de la LOPD, donde se establece que datos de carácter personal serán aquellos datos pertenecientes a personas físicas identificadas o identificables. Es decir, cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. También hemos de hacer referencia a los datos de carácter sensible o especialmente protegidos, esto serán los datos relativos a la ideología, afiliación sindical, religión, creencias, origen racial, **salud** o vida sexual.



Es importante también atender al significado del término ***tratamiento de datos*** al que tanto la LOPD como el RGPD hacen continuamente referencia. Por tratamiento, se entiende cualquier operación que se realice sobre los datos personales, tanto por procedimientos automatizados como por procedimiento no automatizados. Por lo tanto, tratar los datos puede ir desde su registro, organización y estructuración hasta la supresión o destrucción de los mismos.

Aunque son más las partes que integran la relación en el tratamiento de datos, será suficiente con comprender qué se entiende por los siguientes sujetos:

* **Afectado o Interesado**. Por afectado o interesado, debemos de entender a la persona física titular de los datos que sean objeto de tratamiento.

Calle Barceló nº 1, 1º Izda. - 28004 - Madrid - Telf.: 91 532 00 09 - Fax: 91 522 78 94

hya@hebreroyasociados.com

* **El responsable del tratamiento.** Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

* **Encargado del tratamiento.** La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

* **Terceros y otros sujetos.** La persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

## ¿CUÁLES SON LOS PRINCIPIOS QUE DEBERÁN DE GARANTIZARSE EN EL TRATAMIENTO DE DATOS?



Para que el Consejo General de Colegios Oficiales de Podólogos de España pueda tratar datos de sus clientes y/o miembros/asociados se le exigirá que dicho tratamiento cumpla con una serie de principios. Es por ello que el nuevo RGPD establece una serie de principios relativos al tratamiento de datos de carácter personal:

- **Licitud, lealtad y transparencia.** El tratamiento de datos deberá de asegurar que los datos son tratados de manera lícita[1], leal y transparente.

[1] El tratamiento de los datos solamente será lícito cuando cumpla al menos uno de los supuestos establecidos en el RGPD; consentimiento del interesado para uno o varios fines, el tratamiento es necesario para ejecutar un contrato en el que el interesado es parte, el tratamiento es necesario para cumplir una obligación legal aplicable al responsable del tratamiento, cuando dicho tratamiento es vital para proteger intereses vitales del interesado o de otra persona

- **Limitación de la responsabilidad.** Los datos deberán de ser recogidos con fines determinados, explícitos y legítimos, y no podrán ser tratados para fines diferentes para los que fueron recabados.

- **Minimización de los datos.** Los datos deberán ser adecuados, pertinentes y limitados en relación con los fines para los que son tratados. Este principio implica que las empresas deberán obtener los datos mínimos necesarios para el cumplimiento de los fines del tratamiento.

- **Exactitud**. Los datos han de ser exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

- **Limitación del plazo de conservación.** Han de ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.

- **Integridad y Confidencialidad.** Tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.



física, cuando se realice por motivos de interés público o bien cuando el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.

Calle Barceló nº 1, 1º Izda. - 28004 - Madrid - Telf.: 91 532 00 09 - Fax: 91 522 78 94

hya@hebreroyasociados.com

# EL CONSENTIMIENTO

**El consentimiento del interesado o afectado, es uno de los pilares básicos del RGPD.** El Consejo General de Colegios Oficiales de Podólogos de España deberá contar con el consentimiento de sus clientes y/o asociados/miembros para el tratamiento de sus datos. Todo tratamiento llevado a cabo sin el consentimiento del cliente supondrá la ilicitud del mismo. El consentimiento ha de entenderse como *toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.* **Es decir, el consentimiento ha de prestarse de forma EXPRESA para el fin de su tratamiento, y en ningún caso se aceptará el consentimiento tácito correspondiendo al Consejo General de Colegios Oficiales de Podólogos de España probar que el interesado prestó sus datos para ese fin concreto.**



Resulta igualmente importante destacar que el interesado que prestó consentimiento para el tratamiento de sus datos, podrá en cualquier momento retirar ese consentimiento prestado al responsable o al encargado del tratamiento. El reglamento hace hincapié en la importancia de este derecho, estableciendo que retirar el consentimiento deberá de ser igual de sencillo que prestarlo.

Calle Barceló nº 1, 1º Izda. - 28004 - Madrid - Telf.: 91 532 00 09 - Fax: 91 522 78 94

hya@hebreroyasociados.com

## ¿QUÉ NOVEDADES INTRODUCE EL REGLAMENTO EN MATERIA DE DERECHOS A LOS INTERESADOS?

## LOS DERECHOS "ARCOPO"

Los derechos que el interesado ostenta en lo que a la protección de datos se refiere, han venido reconocidos por la LOPD, estableciéndose los comúnmente denominados derechos ARCO. Los derechos ARCO, implican el derecho de acceso a la información, el derecho a rectificar la información, el derecho de cancelación y el derecho de oposición.

El **derecho de acceso** a los datos, implica que el interesado tendrá derecho a acceder a todos los datos de carácter personal que posee el responsable/encargado del tratamiento de los datos y también a conocer el origen de los mismos.



Por su parte, el **derecho de rectificación** implica el derecho que posee el interesado a rectificar aquellos datos que sean incorrectos o que hayan quedado obsoletos.

El **derecho de cancelación**, como su nombre indica, es el derecho que el titular posee para eliminar todos aquellos datos que posea el responsable del tratamiento.

Finalmente, el **derecho de oposición**, establece que el interesado podrá solicita que finalice el tratamiento de sus datos personales, en aquellos casos en los que no haya sido necesario el consentimiento del titular de los datos para su tratamiento y siempre que una Ley no disponga lo contrario.

Calle Barceló nº 1, 1º Izda. - 28004 - Madrid - Telf.: 91 532 00 09 - Fax: 91 522 78 94

hya@hebreroyasociados.com

Con la entrada en vigor del RGPD (25 de mayo de 2016), se reconocen dos nuevos derechos al interesado, cuyo contenido abordaremos a continuación:

**El derecho a la portabilidad de los datos**. Viene regulado en el artículo 20 del RGPD, el cuál reza "*El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado".*

Es decir, mediante el ejercicio del derecho a la portabilidad de datos, el interesado podrá solicitar al encargado del tratamiento para que le facilite todos los datos de carácter personal que figuren en su poder en un formato digital legible. De este modo, el objetivo primordial de la portabilidad de los datos es facilitar el cambio de un proveedor de servicios a otro, reforzando así la competencia entre servicios.



**Derecho al olvido**. Viene regulado en el artículo 17 del RGPD. Mediante el ejercicio de este derecho, el interesado podrá exigir al responsable del tratamiento que se le supriman, sin dilaciones indebidas, todos los datos de carácter personal que le conciernen cuando concurra alguna de las siguientes circunstancias:

- **Cuando no sean necesarios** para los fines por los que se obtuvieron
- Cuando el interesado **retire el consentimiento** prestado
- Cuando el interesado se **oponga al tratamiento** de los mismos
- Cuando el tratamiento de los datos **no cumpla el principio de licitud**
- Cuando deban suprimirse para cumplimiento de una **obligación legal**
- Cuando los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información

## ¿QUÉ SON LOS CÓDIGOS DE CONDUCTA Y LAS CERTIFICACIONES?

Los códigos de conducta y las certificaciones son otra de las importantes novedades que presenta este nuevo Reglamento. Establece el RGPD que las empresas tendrán que adherirse a códigos de conducta con el fin de verificar que estas han cumplido efectivamente con sus obligaciones.

En este sentido, estarán obligados a promover la elaboración de códigos de conducta los Estados miembros, las autoridades de control, el comité y la comisión, cuya finalidad estará destinada a contribuir a la correcta aplicación del reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.



Pero también podrán ser las empresas la que podrán elaborar sus propios códigos de conducta o incluso ampliar los ya establecidos por los EM. De esta manera, siempre y cuando se garantice haber actuado acorde a estos códigos, se estará actuando acorde al RGPD.

En definitiva, la elaboración de códigos de conducta, tiene como principal objetivo lograr que los responsables o encargados- incluidas las AAPP-del tratamiento de datos de carácter personal, cumplan lo dispuesto en el RGPD. Por lo tanto, el cumplimiento del código de conducta podrá servir para demostrar el cumplimiento de las obligaciones del responsable o encargado del tratamiento.

El órgano encargado de garantizar que dichos códigos son efectivamente cumplidos por las empresas, será aquel que determine la Agencia de Protección de datos competente.

Calle Barceló nº 1, 1º Izda. - 28004 - Madrid - Telf.: 91 532 00 09 - Fax: 91 522 78 94

hya@hebreroyasociados.com

Otra de las novedades que el Reglamento presenta, y a las que hay que hacer especial mención, es a la creación de **mecanismos de certificación**. De este modo, el Reglamento establece que los Estados Miembro, las autoridades de control, el Comité y la Comisión, promoverán la creación de mecanismos en de certificación en materia de protección de datos y de sellos y marcas de protección de datos, con la finalidad de demostrar que el responsable o el encargado del tratamiento ha cumplido con todas las obligaciones que el reglamento establece en materia de protección de datos de carácter personal.

Esta certificación, tendrá carácter voluntario y estará disponible a través de un proceso transparente. El nuevo reglamento dispone que las certificaciones tendrán una validez no superior a 3 años, no obstante, matiza que pueden ser renovadas siempre y cuando se sigan reuniendo los requisitos por los cuales fueron otorgadas.



## ¿A QUÉ PAÍSES FUERA DE LA UE PODRÁN LAS EMPRESAS TRANSFERIR LOS DATOS?

Aunque la transferencia internacional de datos ya estaba incluida en el la LOPD, también se hace especial mención a este tema en el Reglamento. La trasferencia internacional de datos, o lo que es lo mismo, la trasferencia de datos a un tercer país es, según lo establecido en el artículo 5.1 del Reglamento de la Ley de Protección de Datos, *"un tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (EEE), bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español".*

Es decir, toda transferencia de datos a un país que no forme parte del Espacio Económico Europeo, será considerada transferencia internacional de datos. Para que esta esté autorizada

por el Reglamento, deberá de garantizarse por la comisión que el destinatario de los datos cumple con un nivel de protección adecuado. Actualmente, son muy pocos los países que por acuerdo de la Comisión cuentan con un nivel de protección adecuado (Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda y Estados Unidos).

No obstante, el reglamento contempla que, a falta de decisión por parte de la Comisión sobre el nivel de protección adecuado, el responsable del tratamiento o encargado del tratamiento podrá transmitir datos personales a un tercer país y organización internacional siempre y cuando ofrezca **garantías adecuadas** y los interesados cuenten con derechos exigibles y acciones legales efectivas.



## ¿QUÉ ES LA EVALUACIÓN DE IMPACTO?
## ¿CUÁNDO ME TENGO QUE SOMETER A ELLA?

El Reglamento obliga en determinados supuestos, a someter a evaluación el impacto que el tratamiento de los datos pueda suponer. En particular estarán obligadas las empresas, cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, entrañe un alto riesgo para los derechos y libertades de las personas físicas. En este supuesto las empresas realizarán, antes de llevar a cabo el tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos. Esta evaluación será especialmente importante en determinados supuestos:

a) decisiones automatizadas, que originen efectos jurídicos hacia el interesado o le afecte significativamente,

b) tratamientos a gran escala de categorías especiales de datos o de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas,

c) observación sistemática a gran escala de una zona de acceso público.

Asimismo, será la Agencia competente la que emitirá un listado de todas aquellas operaciones de tratamiento que hayan de someterse a una evaluación de impacto.

La evaluación de impacto deberá de incluir una descripción sistemática de las operaciones de tratamiento que se vayan a realizar así como el fin del tratamiento, una evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento con respecto a su finalidad, una evaluación de los riesgos que supondrá el tratamiento para los derechos y libertades de los interesados así como las medidas previstas para afrontar los riesgos, las garantías y las medidas de seguridad que habrán de adoptarse para garantizar la protección de datos.



Si tras la evaluación de impacto se determinara que el tratamiento entraña un riesgo alto al que la empresa no pueda hacer frente con las medidas de seguridad a las que tiene acceso, deberá de consultar a la autoridad de control. Esta figura se denomina **consulta previa**, puesto que deberá de consultarse al órgano de control **antes de llevar a cabo el tratamiento** y siempre que, de la evaluación de impacto se derive que el tratamiento supone un riesgo alto no paliable con las medidas de seguridad que nuestra empresa posee. La autoridad de control deberá, en un plazo de 8 semanas desde la realización de la consulta, asesorar por escrito a la empresa responsable del tratamiento.

## ¿QUÉ MEDIDAS DE SEGURIDAD DEBERÁN DE ADOPTAR LOS ENCARGADOS DEL TRATAMIENTO?

El reglamento que desarrolla la LOPD establece de forma muy minuciosa y detallada las medidas de seguridad que deberán de ser aplicadas por las empresas en el tratamiento de los datos, las cuales varían en función del tipo de dato objeto de tratamiento.

Sin embargo, el RGPD no adopta el mismo criterio que establecía el Reglamento, sino que en virtud del riesgo que presente el tratamiento de esos datos, se deberán de adoptar por las empresas todas aquellas **medidas de índole técnica y organizativa** necesarias para garantizar un nivel de protección de seguridad adecuado. Para la adopción de este tipo de medidas, las empresas deberán tener en cuenta determinados factores como son:

- El estado de la técnica.
- Coste de aplicación de las medidas de seguridad.
- Naturaleza, alcance, contexto y finalidad del tratamiento.
- Riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.



En función a esos factores, éstas son algunas de las medidas que las empresas podrán adoptar para asegurar la protección de los datos:

- La seudonimización y el cifrado de los datos;
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamientos;

Calle Barceló nº 1, 1º Izda. - 28004 - Madrid - Telf.: 91 532 00 09 - Fax: 91 522 78 94
hya@hebreroyasociados.com

- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

- Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

En definitiva, antes de adoptar cualquier tipo de medida de seguridad, las empresas deberán valorar el riesgo que entraña el tratamiento de los datos, y una vez determinado y analizado ese riesgo, deberá de llevar a cabo todas aquellas medias técnicas y organizativas que aseguren un nivel de protección adecuado.

## ¿CÓMO CUMPLIR CON EL RGPD?
## DESIGNANDO A UN DELEGADO DE PROTECCIÓN DE DATOS



**El delegado de protección de datos es quizás una las novedades más importantes introducidas en el Reglamento**.

Las empresas (aunque no todas) estarán obligadas a nombrar un delegado de protección de datos. Su principal función será la de asesorar e informar a las empresas de las obligaciones a las que están sujetas en materia de protección de datos, supervisar el cumplimiento de las mismas, asesorar también en materia de evaluación de impacto, cooperar con la autoridad de control y actuar como punto de contacto para todas las cuestiones relativas al tratamiento de los datos.

El reglamento dispone que solamente estarán obligadas a nombrar un delegado de protección de datos si la empresa que los trata es:

- Una autoridad o un organismo de público
- Si la actividad principal de la empresa es el tratamiento de datos sensibles a gran escala o cuando tengan entre sus actividades principales las operaciones de tratamiento que requiera una **observación habitual y sistemática de los interesados a gran escala**.

En *sensu contrario*, hemos de entender que todas aquellas empresas de carácter privado que no tengan como actividad principal el tratamiento de datos o que al menos, no requieran una observancia habitual y sistemática a gran escala, no estará obligados a nombrar un delegado. No obstante, desde nuestro punto de vista sí que sería recomendable ya que a través de esta figura las empresas podrán cumplir con creces las obligaciones establecidas por el RGPD, evitando la imposición de multas por incumplimiento.



## EL NUEVO RÉGIMEN DE SANCIONES EN EL RGPD

Otra novedad introducida por este reglamento es el nuevo sistema de infracciones y sanciones. Toda empresa que no cumpla con las obligaciones establecidas en el reglamento estará obligada, además de a resarcir los daños ocasionados al interesado, a soportar multas administrativas que podrán alcanzar hasta los 20 millones de euros o incluso hasta el 4% de la facturación de la incumplidora.

Calle Barceló nº 1, 1º Izda. - 28004 - Madrid - Telf.: 91 532 00 09 - Fax: 91 522 78 94
hya@hebreroyasociados.com

El anteproyecto de ley orgánica de protección de datos presentado en junio, clasifica las infracciones, en función de la gravedad del incumplimiento, en muy graves, graves y leves. También se establece un plazo de prescripción para cada una de ellas, siendo de 3 años para las muy graves, 2 años para las graves y de 1 año para las leves.

## RESUMEN DE ASPECTOS CLAVE

**¿Quiénes están obligado al cumplimiento del RGPD y cuándo será exigible su cumplimiento?**

Estarán obligadas todas las empresas que tengan un establecimiento dentro de la UE y también aquellas que, sin tenerlo, presten sus servicios en la UE a ciudadanos residentes. Su cumplimiento será exigible a partir del 25 de mayo de 2018.



**¿Qué implica el contenido mínimo de la información?**

El contenido mínimo de información, hace alusión a uno de los principios fundamentales que ha de cumplirse en el tratamiento de datos. Implica que los datos obtenidos por las empresas han de ser no más de los necesarios para la consecución del fin para el que se recaba. Por ello se exige que sean adecuados, pertinentes y limitados.

**¿Qué factores he de tener en cuenta para aplicar las medidas de seguridad?**

Son muchos los factores que se deben tener en cuenta para la adopción de las medidas de seguridad; El estado de la técnica, los costes de aplicación de las medidas, la finalidad del tratamiento, riesgos que supone el tratamiento, etc.

Calle Barceló nº 1, 1º Izda. - 28004 - Madrid - Telf.: 91 532 00 09 - Fax: 91 522 78 94
hya@hebreroyasociados.com

**¿Qué medidas deberán de adoptar las empresas para hacer frente a los riesgos del tratamiento?**

Una vez han sido detectados los riesgos a los que las empresas se exponen, estas deberán de llevar a cabo todas las medidas de índole técnica y organizativa que garanticen la seguridad del tratamiento como pueden ser la seudonimización o el cifrado de los datos.

**¿Qué hacer tras una evaluación de impacto negativa?**

La evaluación de impacto "negativa" implica que el tratamiento de los datos posee un riesgo alto y que la empresa no posee las medidas de seguridad adecuadas para hacer frente a ese riesgo. En estos casos, antes de efectuar el tratamiento, la empresa deberá solicitar asesoramiento a la autoridad competente.



**El presente informe, que se extiende en dieciocho (18) folios de papel común, se expide en Madrid, a 28 de marzo de 2018, a petición del CONSEJO GENERAL DE COLEGIOS OFICIALES DE PODÓLOGOS DE ESPAÑA.**

**HEBRERO & ASOCIADOS**

Para ampliar información sobre el presente informe pueden dirigirse a:

**HEBRERO & ASOCIADOS**

C/ Barceló nº 1 - 1º Izda., 28004, Madrid

Teléfono: 91 532 00 09

Fax: 91 522 78 94

Mail: hya@hebreroyasociados.com

**Les rogamos que citen siempre nuestra referencia: 5497**