NOVEDADES DEL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS OBLIGATORIAS A PARTIR DEL 25 DE MAYO DE 2018.

Índice de contenido

Nota previa informativa

El nuevo Reglamento General de Protección de Datos (RGPD) será obligatorio a partir del viernes 25 de mayo. Puede que en un futuro a medio plazo se concreten ciertos aspectos mediante una ley estatal. En ese caso, actualizaremos a medida que se publiquen nuevas modificaciones legislativas.

Este documento está redactado pensando en un sector de nuestra clientela: el profesional sanitario que ejerce por cuenta propia.

Toda la información contenida en esta circular es meramente orientativa. No sustituye ningún plan de protección de datos ni sirve para cumplir con los requisitos mínimos exigidos. Aconsejamos que se acuda a empresas especializadas para la llevanza de la protección de datos por tres razones:

1) El profesional por cuenta propia puede disponer de poco tiempo libre para preocuparse por la recogida y el tratamiento de datos de manera exacta, responsable y legal.
2) Aun cuando dispusiera de tiempo, puede suponerle una tarea ardua y extraña a su área profesional.
3) Al igual que un profesional por cuenta propia contrata servicios externos como la contabilidad o la limpieza, la protección de datos puede encuadrarse en este tipo de servicios externos.

Si a pesar de todo, un profesional sanitario quiere llevar su propia protección de datos, puede hacerlo legalmente. No es obligatorio contratar ninguna empresa especializada. Si se prefiere contratar los servicios de empresas especializadas, se debe tener en cuenta que hay una gran oferta en el mercado, por lo que es recomendable preguntar y comparar precios y servicios ofrecidos.

La información que viene a continuación sirve para conocer mejor y con más profundidad los cambios y las novedades que trae el RGPD para poder así tomar mejores decisiones.

Por otra parte, desaconsejamos hacer adaptaciones o descargar plantillas de documentos de seguridad o de la evaluación de impacto sobre la protección de datos, ya que cada clínica sanitaria, cada negocio, es único y tiene unas características especiales. Realizar un copia-pega solo puede traer problemas en un futuro. Esto no contradice que se incluya en este documento u modelo de cláusula de recogida de datos.

Por último, añadiremos que todo lo contenido en esta circular se basa en el RGPD y en documentación e información de la Agencia Española de Protección de Datos (AEPD).

Resumen de novedades

***Supresión de la obligación de inscribir ficheros en la AEPD y de las auditorías bienales.**

Ya no hay que dirigirse a la AEPD para inscribir fichero alguno. A partir de ahora la AEPD ya no cumple la función tuitiva que llevaba desempeñando en los últimos años; pasa a desempeñar una labor meramente de control y punitiva. Del mismo modo, ya no existirá la obligación de realizar auditorías bienales.

***Ampliación de los derechos ARCO.**

Hasta ahora, los interesados tenían cuatro derechos que podían ejercer ante el empresario. Eran los llamados derechos ARCO (acceso, rectificación, cancelación y oposición). A partir de ahora se amplían a tres más: supresión o derecho al olvido, portabilidad, y limitación en el tratamiento[1]. Los profesionales sanitarios deben estar atentos al ejercicio por parte de un paciente de cualquiera de esos derechos.

***Consentimiento explícito.**

El consentimiento del titular de los datos (paciente) será siempre explícito, ya no cabe el consentimiento tácito o por omisión. Se deberá probar que se informó adecuadamente y se obtuvo el consentimiento. El nuevo Reglamento actualiza la minoría de edad a los 13 años para consentir y ejercitar derechos.

***Deber de información.**

La información a los pacientes debe proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. Se debe informar acerca de los siguientes extremos:

-Los datos de contacto del responsable y en su caso, del Delegado de Protección de Datos (DPD)[2].

-Los fines del tratamiento a los que se destinan los datos personales: asistencia sanitaria, publicidad, fines científicos, etc. En caso de que concurran varios, deben enumerarse y detallarse por separado para que el interesado dé el consentimiento para cada uno.

-La base jurídica del tratamiento. Hay varios tipos. En el caso del profesional sanitario, se denomina interés legítimo.

[1] A lo largo de este documento y en todos aquellos que hagan referencia a la Protección de Datos, la palabra "tratamiento" hace referencia al tratamiento de datos, no a tratamiento sanitario.

[2] Se tratará más adelante.

-El plazo de conservación de la información: 5 años en el caso de los profesionales sanitarios por su relación contractual con los pacientes más otros 3 años en caso de bloqueo, es decir, por protección de datos. Por tanto, un plazo total de 8 años.

-Los derechos ARCO, supresión/olvido, portabilidad y limitación en el tratamiento.

-La existencia, en su caso, de decisiones automatizadas o de elaboración de perfiles.

-La previsión, en su caso, de transferencia de los datos a terceros países.

-El derecho a presentar una reclamación ante la AEPD.

La forma de recogida de información puede ser oralmente, por escrito, mediante formularios *on line*, telefónicamente, etc.

***Delegado de Protección de Datos (DPD)**

Esta figura solo será obligatoria en algunos casos. El único caso que afectaría a un profesional sanitario es aquel en que la actividad principal consista en el tratamiento a gran escala de categorías especiales de datos personales[3], como son los referentes a la salud.

El tratamiento de datos personales no debe considerarse a gran escala si lo realiza, respecto de datos personales de pacientes o clientes, un solo médico u otro profesional de la salud[4].

Por tanto, estas dos referencias del RGPD sobre el tratamiento de datos de salud a gran escala y su definición, nos hace llegar a la conclusión de que, a día de hoy, no será obligatorio designar un DPD a menos de que el tratamiento de datos sea a gran escala (tipo hospital o cadenas de clínicas).

***Responsable y encargado del tratamiento.**

El responsable del tratamiento es la persona física o jurídica que determina los fines y los medios del tratamiento. Es decir, el profesional que ejerce por cuenta propia o la entidad mercantil.

El encargado es la persona física o jurídica que realice un tratamiento de datos personales por cuenta del responsable del tratamiento. Por tanto, cuando el responsable contrata una empresa para realizar el tratamiento, ésta será una encargada que realizará el tratamiento por encargo del responsable.

Dicho de otra manera, la obligación de tratar de manera adecuada los datos personales sigue recayendo en el profesional por cuenta propia o empresa sanitaria, que será responsable del fichero de todos los datos personales relacionados con su negocio. Si encarga a una empresa o

[3] Art. 37.1 c) RGPD

[4] Considerando 91 RGPD

despacho especializado dicho tratamiento, ésta será la encargada. Si lo lleva él mismo, será además de responsable, encargado.

***Valoración o análisis del riesgo.**

Todos los responsables deben realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo. El tipo de análisis variará según los tipos de tratamiento, la naturaleza de los datos, el número de interesados (pacientes) afectados, la cantidad y variedad de tratamientos que una misma empresa lleve a cabo.

***Registro de operaciones o de actividades del tratamiento.**

Los responsables y encargados deben mantener un registro de operaciones de tratamiento en el que se contenga la información que establece el RGPD.

Los registros deben constar por escrito, pudiendo ser en formato electrónico. El registro debe estar a disposición de la AEPD en caso de requerimiento.

En el siguiente apartado se explicará con detenimiento el contenido del registro de actividades con una doble finalidad: ilustrativa y orientativa. Es un contenido mínimo, es decir, todo lo que se pueda ampliar y personalizar adecuándolo a las circunstancias particulares será positivo.

Contenido del registro de actividades

1. Nombre y datos de contacto del responsable, del representante del responsable (en caso de sociedad, el administrador) y del delegado de protección de datos, en su caso.

2. Fines del tratamiento.

3. Descripción de las categorías de interesados y de las categorías de datos personales.

4. Categorías de destinatarios a quienes se comunicarán los datos personales.

5. Transferencias de datos personales a un tercer país o a una organización internacional.

6. Plazos previstos para la supresión de los datos.

7. Descripción general de las medidas técnicas y organizativas de seguridad.

8. Registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un encargado. Debe contener:

-El nombre y datos de contacto del encargado y del responsable por cuenta del cual actúe el encargado, y en su caso, de representante del responsable o del encargado, y del delegado de protección de datos.

-Las categorías de tratamientos efectuados por cuenta de cada responsable.

-Las transferencias de datos personales a un tercer país u organización internacional.

-La descripción general de las medidas técnicas y organizativas de seguridad.

A continuación, un ejemplo de campos que componen el registro de actividades del tratamiento. En sombreado rojo aparecen aquellos campos que no serán aplicables a la mayoría de las unidades asistenciales.

RESPONSABLE DEL TRATAMIENTO

Responsable del tratamiento	Nombre y datos de contacto del responsable o representante del responsable, en su caso.
Delegado de Protección de Datos	Nombre y datos de contacto del DPD, en su caso.
DESCRIPCIÓN DE LA ACTIVIDAD	
Actividad de tratamiento	Conjunto de operaciones, procesos, protocolos que conlleven recogida, consulta, grabación, modificación, cesión, o destrucción de datos de carácter personal.
Finalidad	Descripción de los fines explícitos y la fundamentación jurídica para proceder a la realización de actividades de tratamiento sobre datos personales.
Interesados	Categoría de personas físicas identificadas o identificables.
Categoría de los datos	Detalle de los datos identificativos, biométricos, de salud…
Período de conservación	Indicador de los plazos de conservación de la información establecidos en función del tratamiento, la finalidad, la categoría del dato y las leyes. El plazo general para pacientes será de 8 años (5 años de prescripción de la responsabilidad más 3 de bloqueo).
Medidas de seguridad	Descripción de las medidas técnicas y organizativas de seguridad: sistema informático, ordenadores, videovigilancia, llaves, discos duros extraíbles, armarios, rejas, alarmas, etc.
TRANSFERENCIAS Y CESIONES	
Cesiones	Categorías de destinatarios a quienes se comunicarán los datos personales.
Transferencias de datos internacionales	Identificación de transferencias internacionales, país u organización. Consentimiento explícito del interesado, etc.
ENCARGADO DEL TRATAMIENTO	
Encargado del tratamiento	Nombre y datos de contacto del encargado.
DPD	Nombre y datos de contacto del DPD, en su caso.
Responsable del tratamiento	Nombre y datos del responsable por cuenta del cual actúe
Categorías de tratamiento	Operaciones, procesos, protocolos que conlleven recogida, consulta, grabación, modificación, cesión, o destrucción de datos de carácter personal.
Transferencia de datos internacionales	Identificación de transferencias internacionales, país u organización. Consentimiento explícito del interesado, etc.
Medidas de seguridad	Descripción de las medidas técnicas y organizativas de seguridad.

Cláusula informativa de recogida y tratamiento de datos

Se presenta a continuación un modelo de cláusula informativa sobre la recogida y el tratamiento de datos para insertar en la ficha del paciente cuando se le recojan sus datos por primera vez. Si se recogen los datos por página web, es mejor utilizar un consentimiento por capas, tal y como se explica en la guía de la AEPD anexada.

D./Dña. [Nombre del Paciente] AUTORIZA expresamente a que sus datos de carácter personal, y cualquier otro dato de esa índole que sea necesario, sean tratados por [Nombre de la clínica] con el fin de prestarle el servicio sanitario más adecuado y realizar la facturación de éste. Los datos proporcionados se conservarán mientras se mantenga la relación contractual o durante los años necesarios para cumplir con las obligaciones legales, que en el caso del tratamiento de datos sanitarios es de ocho años, cinco por ser el plazo de prescripción de la responsabilidad y tres de bloqueo de datos por las autoridades competentes. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal.

Usted tiene derecho a obtener confirmación sobre si [Nombre de la clínica] está tratando sus datos personales, a acceder, rectificar, y suprimir los datos, solicitar la portabilidad de los mismos, oponerse al tratamiento y solicitar la limitación de éste, tal y como recoge el Reglamento General de Protección de Datos

La legitimación del tratamiento es la relación contractual y el cumplimiento de las obligaciones profesionales y legales derivadas de la misma.

En ____, a ___ de ____ de 20__

Fdo. Fdo.

Anexo

Se adjunta enlace web para acceder a la "Guía para el cumplimiento del deber de informar" elaborada por la AEPD, por si fuera de interés para algún colegiado ampliar sus conocimientos sobre esta cuestión.

http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf

En Sevilla, a 21 de mayo de 2018.

Desler
Abogados

Elena Sánchez Castro

Abogada