Boletín 11/18

LOPD EN LA EMPRESA

Aselio | PROTECCIÓN DE DATOS

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

EL RGPD UE 2016/679 EN APLICACIÓN

El Consentimiento del Interesado (I)

El tratamiento de los datos personales por parte de un responsable será lícito siempre y cuando cumpla alguna de las condiciones que se recogen en el art.6. Este artículo se constituye como uno de los más importantes del RGPD.

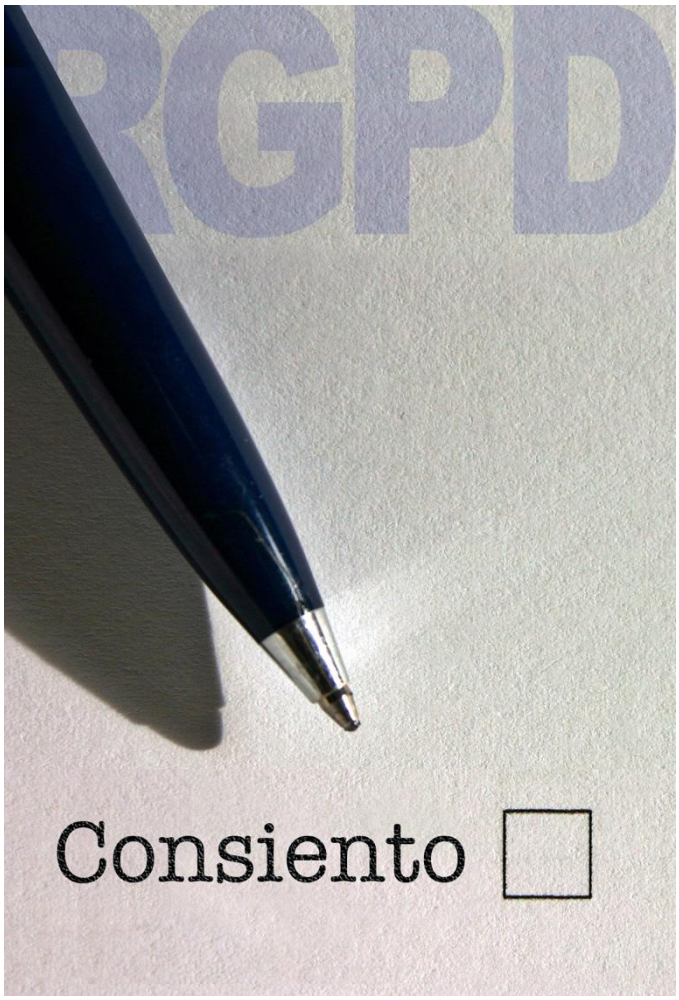
Una de las condiciones que legitiman el tratamiento es el Consentimiento. A lo largo del articulado del reglamento podemos encontrar pistas de **cómo, cuándo y para qué hemos de pedirlo.** En la actualidad, con la aplicación del RGPD, debemos ser más cuidadosos en cuánto a cumplir con esta licitud, así, por ejemplo, **hoy en día es imposible contemplar un consentimiento tácito** del interesado. Principalmente, tenemos que conocer y tener en cuenta **las características de cómo ha de ser esa manifestación de voluntad:**

a) **Libre**
b) **Inequívoca**
c) **Informada**

El interesado podrá manifestar su voluntad, por ejemplo, mediante una declaración por escrito, marcando una casilla en blanco de un formulario.

El responsable, además, tendrá que cumplir con la obligación de informar del tratamiento de los datos personales, basados en ese consentimiento.

Contenido



IMPORTANTE

El consentimiento para el tratamiento de **datos sensibles, la toma decisiones automatizadas o transferencias a terceros países, requiere de un consentimiento inequívoco y explícito.**

SANCIONES DE LA AEPD

LA AEPD ACLARA

Web sancionada por utilizar dispositivos de almacenamiento y recuperación de datos sin informar al interesado

Tratamiento de los datos personales de los menores de edad en los historiales clínicos

En el procedimiento sancionador PS00372-2016, la Agencia Española de Protección de datos **sanciona a la entidad ALBEHAS.PT LIMITED por la infracción del art.22.2 de la Ley de Servicios de la Sociedad de la Información (en adelante, LSSI).**

Con fecha 13 de febrero de 2016, los denunciantes, **varias asociaciones de derechos de autor, presentaron un escrito alegando que la entidad denunciada era la responsable de la página web lolabits.es**, la cual incumplía con la información prevista del art.5 LOPD, así como el envío de publicidad sin posibilidad de oposición y la descarga e instalación de cookies sin información.

A la vista de los hechos denunciados la AEPD, en fase de actuaciones previas, realizó la práctica de diligencias y pruebas acordando las siguientes conclusiones:

Con fecha 23/03/2016 se verificó que la web lolabits.es utiliza dispositivos de almacenamiento y recuperación de datos, en adelante DARD, con la finalidad de analítica web de tercera parte y para la gestión de redes sociales; y que incluye un sistema de información, con una primera capa sin especificar las finalidades de los DARD utilizados y con una segunda capa que **no hace referencia al almacenamiento local relativo a redes sociales**, vulnerando, por lo tanto, el contenido del art.22.2 de la LSSI, aplicable a todo tipo de DARD, y que incluye no solamente las cookies, sino cualquier otra tecnología similar.

La Agencia Española de Protección de datos en la 10ª Sesión Anual, informa que los requisitos aplicables al consentimiento informado para el uso de las cookies serán los establecidos en el RGPD.

IMPORTANTE

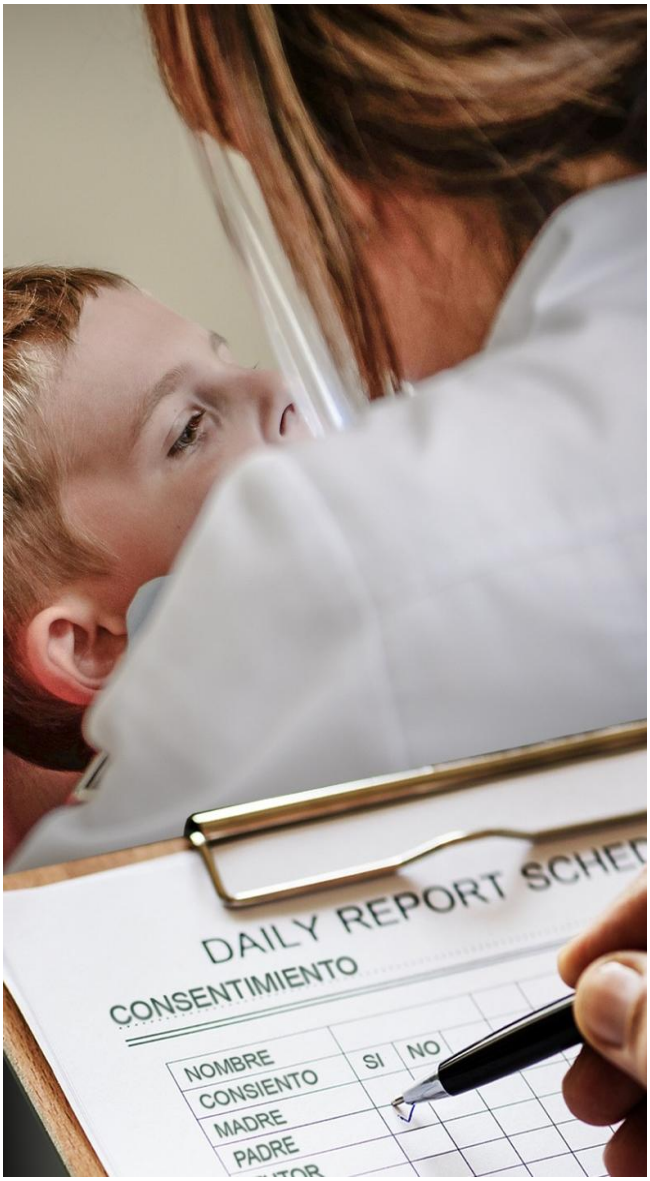
Con el fin de garantizar la utilización de los dispositivos de almacenamiento con fines legítimos, **la normativa comunitaria y nacional exige de un consentimiento informado del usuario.**

El informe 2014-222 **resuelve acerca del tratamiento de los datos personales de los menores de edad en los historiales clínicos,** aplicando la aún vigente ***Ley Orgánica 15/1999 de 13 de diciembre, de Protección de datos de carácter personal, y su Reglamento de desarrollo 1720/2007.***

En el art.13.1 del citado Reglamento nos dice que se procederá **al tratamiento de los datos de los mayores de catorce años con su consentimiento**, salvo en aquellos casos en los que la ley exija para su prestación la asistencia de los padres o tutores legales. **En el caso de los menores de catorce años se requiere el consentimiento de los padres.**

La *Ley 41/2002 básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación pública* señala los supuestos en los que **el consentimiento será prestado por los representantes legales, cuando el paciente menor de edad no sea capaz intelectual y emocionalmente de comprender el alcance de la intervención médica,** no aplicándose por lo tanto el art.13.1 del reglamento.

Además, **el ejercicio del derecho de acceso de los padres/tutores al historial clínico de los menores**, emancipados o no, está amparado en el Código Civil, que habilita la cesión del historial clínico para ejercer la salvaguarda del menor.



IMPORTANTE

El menor de edad mayor de catorce años podrá ejercitar por si solo el derecho de acceso a su historial clínico, **no pudiendo oponerse a que sus padres o tutores legales ejerzan ese mismo derecho.**

ACTUALIDAD LOPD

Riesgos a los que puede enfrentarse la labor del Delegado de Protección de Datos

Fuente: AEPD

En un artículo anterior abordamos la figura del Delegado de Protección de Datos (DPD) cuando se construyen sistemas de información en las organizaciones, centrándonos en la planificación. El Plan de Sistemas de Información de una organización tiene como propósito establecer un marco de referencia para los sistemas, para que su desarrollo y evolución sea coherente, y a la vez esté alineado con los objetivos estratégicos de la organización. Es, por tanto, una parte de la planificación estratégica que guiará la evolución del negocio a medio y largo plazo.

Como se comentaba entonces, el DPD debe participar en la elaboración de este Plan de Sistemas, asesorando e informando de las obligaciones que impone el Reglamento General de Protección de Datos (RGPD) en el tratamiento de datos personales. La propia organización debe promover esta participación a lo largo de toda la planificación estratégica para que el DPD se involucre desde las fases más tempranas, ayudando a crear también una cultura de la protección de datos en la organización. No hay que olvidar que el artículo 25 del RGPD incluye la protección de datos desde el diseño, y ese diseño se puede considerar que empieza desde la visión estratégica de la organización.

Puede ver más información en el siguiente enlace:

La figura del DPD

El DPD en las Administraciones públicas.

EL PROFESIONAL RESPONDE

Qué son las brechas de seguridad, detección y clasificación

Los responsables del tratamiento y en su caso los encargados del tratamiento, cuando así se haya establecido en el contrato, **desde el momento en que tengan el conocimiento de una brecha de seguridad que suponga un riesgo para los derechos y libertades de las personas, deben de** notificarlo a la autoridad competente lo más rápido posible y **dentro del plazo de las 72 horas siguientes a tener constancia del hecho.**

En esa notificación deberá indicarse como mínimo:

- **La naturaleza de la quiebra de seguridad** (confidencialidad, disponibilidad o integridad).
- **Categorías de datos, número aproximado de interesados** afectados (si fuera posible).
- **Categorías y número aproximado de registros de datos** personales afectados.
- **Comunicar el nombre y datos de contacto del DPD** u otra persona para obtener información.
- **Describir las consecuencias** de la quiebra de seguridad de los datos personales.
- **Describir las medidas adoptadas o propuestas por el responsable**, para poner remedio o en su caso mitigar los efectos negativos.

IMPORTANTE

Si no fuera posible facilitar toda la información en 72 horas, **se podrá hacer de forma gradual sin dilación indebida**. Toda la información debe ir documentada.