

LA LOPD EN EL DÍA A DÍA

Cuándo aplicar medidas de seguridad de nivel Alto

Establece el artículo 81 RDLOPD, que deberán aplicarse, las medidas de seguridad de **nivel ALTO** a los ficheros y tratamientos de datos personales cuando:

- a) Se refieran a la **ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual** de una persona, salvo que dichos datos se utilicen sólo para realizar transferencias dinerarias a entidades de las que los afectados sean miembros; que se trate de ficheros en papel en los que aparezcan estos datos de forma accesorio; o que se trate de datos como el grado de discapacidad, la declaración de la condición de discapacidad o invalidez del afectado para el cumplimiento de determinados deberes públicos. En estos casos, bastará aplicar medidas de seguridad de nivel BÁSICO.
- b) Contengan o se refieran a **datos recabados para fines policiales sin consentimiento** de los afectados.
- c) Contengan **datos derivados de actos de violencia de género**.
- d) Contengan **datos de tráfico y localización** cuyos responsables sean operadores de servicios de comunicaciones electrónicas.

Estas entidades deberán llevar un registro de accesos.

Contenido

Cuándo aplicar medidas de seguridad de nivel Alto	1
Sanción por no atender al derecho de oposición	2
Tratamiento y publicación de datos en foro	3
La AEPD informa al Grupo de Autoridades europeas	4
¿Podemos comunicar datos sanitarios de una persona...	5



IMPORTANTE

La aplicación de las medidas de seguridad de nivel ALTO implica que deberán aplicarse además, las de **nivel MEDIO Y BÁSICO**.

SANCIONES DE LA AEPD**Sanción por no atender al derecho de oposición**

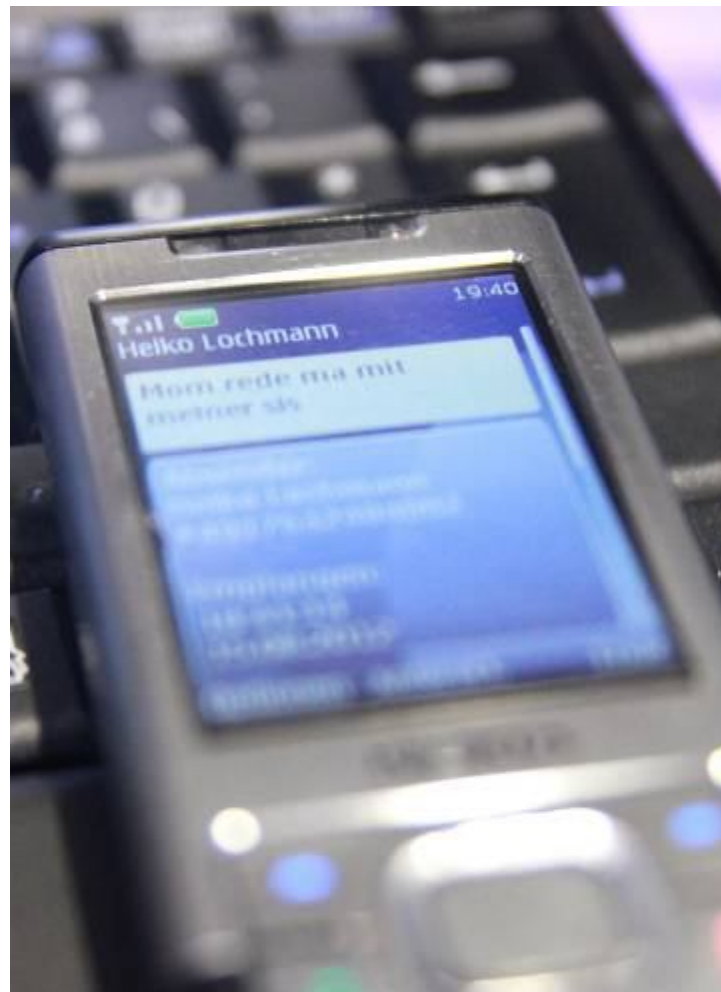
En el procedimiento sancionador [PS/00399/2015](#) de la AEPD observamos la sanción que recibe una empresa energética **por no atender debidamente el derecho de oposición** al tratamiento de los datos con fines publicitarios.

En marzo de 2015 tiene entrada en la Agencia un escrito en el que el denunciante declara que **a pesar de haber ejercitado ante la energética su derecho de oposición** al tratamiento de sus datos para fines publicitarios, **ha seguido recibiendo** en su teléfono móvil mensajes SMS comerciales, no sólo de dicha entidad, sino también una carta con publicidad de Cofidis.

Ante los hechos denunciados, los Servicios de Inspección de la Agencia solicitan información a la entidad Responsable, manifestando esta que pese a que en sus sistemas, **los datos del denunciante se habían marcado dentro de la lista Robinson** para evitar el envío de publicidad y cesión de sus datos a otras empresas del grupo, **el envío del SMS publicitario se debía a un error en la actualización de sus bases de datos** con fines publicitarios.

Resultado: multa de 5.000 €, por infracción del artículo 21.1 de la LSSI, tipificada como leve en el artículo 38.4.d) de la misma, de conformidad con los artículos 39.1.c) y 40 de la citada LSSI.

La empresa responsable debe atender los requerimientos de derechos ARCO de forma efectiva.

**IMPORTANTE**

El responsable deberá mantener los datos exactos y puestos al día, de forma que respondan con veracidad a la situación actual del afectado.

LA AEPD ACLARA

Tratamiento y publicación de datos en foro



El Informe [0023/2010](#) de la AEPD resuelve la consulta planteada sobre si de conformidad con lo dispuesto en la Ley Orgánica 15/1999, **para el tratamiento y publicación de datos personales en el foro** creado en la página web de una Asociación de enfermos, **es necesario incluir una cláusula informativa** que recoja la política de privacidad de la Asociación.

Ante esta consulta, la Agencia manifiesta que **no solo la recogida de datos a través del foro supone la obligación informar**, sino que además, **es necesaria la obtención del consentimiento expreso de los usuarios del foro para el tratamiento o cesión de sus datos personales que tuvieran el carácter de "sensibles"**, pues dado que se trata de un foro de afectados por una enfermedad, es muy posible que se traten datos de salud, por lo que el consentimiento deberá recabarse de forma que sea imposible introducir cualquier dato sin que previamente el afectado haya conocido la información exigida en el artículo 5 de la LOPD. Puede servir **como prueba de dicho consentimiento, que la web impida introducir los datos personales, sin que el participante haya aceptado el aviso legal.**

Por tanto, **no solo es obligado insertar el aviso legal en el blog, sino que es conveniente que se incluya una casilla que pueda ser la prueba de que se ha obtenido el consentimiento expreso** e informado del interesado, tanto para el tratamiento como para la publicación de los datos en el blog.



IMPORTANTE

Es obligación del responsable del fichero o tratamiento conservar el soporte en el que se acredite que cumplió con el deber de informar.



ACTUALIDAD LOPD

La AEPD informa al Grupo de Autoridades europeas de protección de datos de los avances en relación a la política de privacidad de Google

Fuente: www.agpd.es

La Agencia ha constatado que Google ha introducido modificaciones significativas en materia de información, consentimiento y ejercicio de derechos, áreas sobre las que la AEPD le requirió que hiciese cambios. La compañía se ha comprometido a adoptar medidas adicionales específicamente solicitadas por la Agencia y a mantener un diálogo constante.

- La Agencia ha examinado la evolución en el último año de la política de privacidad de Google, en el marco del seguimiento de la resolución sancionadora hecha pública hace dos años
- La AEPD ha constatado que la compañía ha introducido modificaciones significativas en materia de información, consentimiento y ejercicio de derechos, áreas sobre las que la AEPD le requirió que hiciese cambios
- Google también se ha comprometido a adoptar medidas adicionales específicamente solicitadas por la Agencia y a mantener un diálogo constante tanto sobre la aplicación de nuevas medidas como a informar de futuros cambios que puedan afectar a la privacidad de los ciudadanos

(Madrid, 11 de enero de 2016). La Agencia Española de Protección de Datos (AEPD) ha participado recientemente en la reunión plenaria del Grupo de Autoridades europeas de protección de datos (GT29). El Grupo analizó, entre otros temas, los avances realizados en los **procedimientos nacionales abiertos** respecto a la política de privacidad unificada puesta en marcha por Google en 2012. En el caso español, [el procedimiento concluyó](#) en diciembre de 2013 declarando la existencia de tres infracciones graves de la normativa de protección de datos, imponiendo una sanción de 900.000 euros y realizando un requerimiento a la compañía para que adoptase las medidas necesarias para ajustar su política de privacidad a la normativa española.

La AEPD comunicó al Grupo que ha estado examinando la evolución en el último año de la política de privacidad de Google. En este sentido, la Agencia ha constatado que, con posterioridad a la resolución y tal y como se le requería en la misma, la compañía ha introducido [modificaciones significativas](#) en materia de información ofrecida a los usuarios, consentimiento y ejercicio de derechos, áreas en las que se centraban los incumplimientos detallados en el procedimiento sancionador de la AEPD y sobre las que se le instaba a hacer cambios.

Algunas de las **medidas puestas ya en marcha** por la compañía a solicitud de la Agencia Española son las siguientes:

- Se ha habilitado el centro "Información personal y privacidad" a partir del enlace "Mi cuenta" a los usuarios con cuenta en Google, donde se ofrece información adicional y opciones de gestión de la información recogida por Google, con algunas posibilidades de gestión también para usuarios no autenticados.

Puede ver más información en el siguiente enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_01_11-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Podemos comunicar datos sanitarios de una persona atendida de urgencia a familiares o allegados?

Cuando se produce una asistencia sanitaria de urgencia a una o varias personas que han tenido un accidente y han sido trasladadas a un hospital, **¿puede la entidad responsable del tratamiento (el hospital o el 112) comunicar esta información a las personas que llaman por teléfono para interesarse, sin vulnerar la LOPD?, o ¿se ha de pedir el consentimiento del paciente?**

La respuesta depende de la información que se ofrezca al familiar o allegado solicitante.

Debido a que puede tratarse de información relacionada con la salud del accidentado, en principio sería necesario el consentimiento expreso del paciente para poder comunicar sus datos, **salvo que exista una norma con rango de Ley así lo establezca.**

Al respecto, la propia Ley permite una **excepción a esta regla** general, y es **cuando el tratamiento de los datos sea necesario para salvaguardar un interés vital del afectado o de otra persona.**

En estos casos, los servicios de urgencias y emergencias responsables del tratamiento de datos de personas que allí llegan, **podrán comunicar a quienes soliciten información sobre si éstas han sido o no atendidas, del hospital al que han sido trasladadas e incluso sobre su estado de salud sin vulnerar la LOPD,** pues es posible que ellos puedan aportar información de interés vital de los atendidos que puede ser necesaria para prestarles una asistencia sanitaria adecuada.

Sin embargo, cualquier otra información que se les ofrezca, podría ser considerada excesiva en relación con el art. 4 LOPD.

**IMPORTANTE**

La cesión de datos sin el previo consentimiento del titular es una de las infracciones más graves en el cumplimiento de la LOPD.