Boletín 07/2016
LOPD EN LA EMPRESA
Autor: Julio César Miguel Pérez
Balaguer & Gutiérrez
Correduría de Seguros
Consultoría de Protección de Datos

LA LOPD EN EL DÍA A DÍA

Cuándo puedo denegar el derecho de acceso

El derecho de **acceso es el derecho del afectado a obtener información sobre si sus propios datos** de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información sobre el origen de dichos datos y las comunicaciones o cesiones realizadas de los mismos.

El responsable del fichero o tratamiento podrá denegar el acceso en estos casos:

a) **Cuando la solicitud sea formulada por una persona distinta del afectado** y no se acredita que actúa en representación de aquél.

b) **Cuando el derecho ya se ha ejercitado en los doce meses anteriores a la solicitud**, salvo que se acredite un interés legítimo al efecto.

c) **Cuando lo prevea una Ley** o una norma de derecho comunitario.

Es decir, de forma general, el titular de los datos solo podrá solicitar **un derecho de acceso una vez cada 12 meses**.

Fuera de estos tres casos, el responsable está obligado a atender el derecho de Acceso incluso aunque no posea datos del solicitante.

Contenido

IMPORTANTE

El responsable del fichero dispone de **un mes** para estimar la solicitud de acceso, y cuenta con **10 días para responder a dicha solicitud** una vez estimada.

SANCIONES DE LA AEPD

Sanción por publicar datos sensibles en la web

El tratamiento de datos de salud requiere el consentimiento expreso de sus titulares

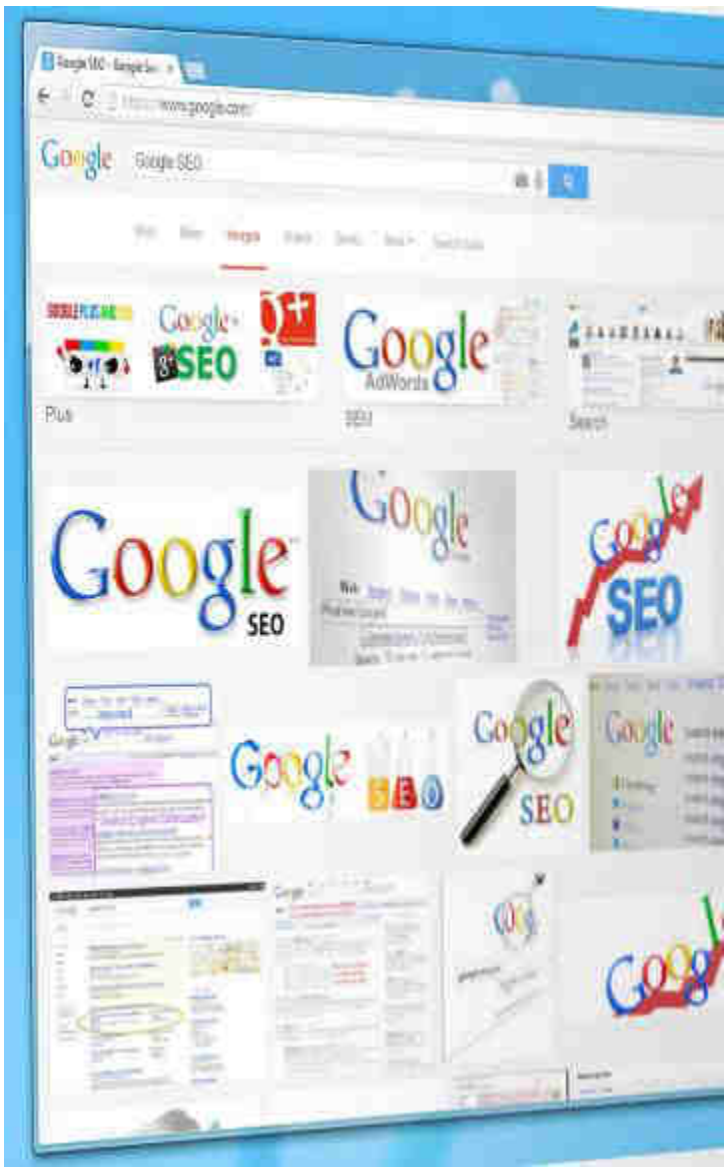
En el PS/00691/2015 de la AEPD podemos ver la sanción impuesta por la AEPD a la Asociación PNM de Madrid **por divulgar documentación con Datos especialmente protegidos a través de su página web**.

El 21/01/2015 tiene entrada en la AEPD un escrito de la Asociación 11 M Afectados de Terrorismo, declarando que el hijo de uno de sus socios, realizando un ejercicio práctico de informática, insertó su nombre y apellidos en Google para ver qué información aparecía sobre él y en qué páginas web. El alumno comprobó que **en una de ellas aparecían publicados libros de familia, informes médicos, informes de autopsias, minusvalías y amputaciones y otra documentación** de las personas implicadas en el atentado del 11 de marzo de 2004, incluida la suya.

A la vista de los hechos, los Servicios de Inspección de la AEPD realizan una búsqueda en la web de la denunciada, la cual **permitía el acceso a documentos del sumario de un proceso judicial**, entre otros.

La AEPD estimó que este tratamiento de datos está sujeto a normativa LOPD y puesto que la APNM no pudo acreditar la recogida del consentimiento de los afectados para el tratamiento y publicación de sus datos, la Directora resuelve sancionar a la demandada.

Resultado: multa de 100.000€ a la Asociación PNM por infracción del artículo 7.3 de la LOPD tipificada como muy grave en el artículo 44.4b) de la misma.



IMPORTANTE

La publicación de datos a través de internet sin consentimiento, es una infracción muy grave en el cumplimiento de la LOPD.

LA AEPD ACLARA

Cesión de imágenes por las Fuerzas y Cuerpos de Seguridad del Estado a entidades bancarias

El Informe Jurídico 156/2014 resuelve la consulta **sobre si las Fuerzas y Cuerpos de Seguridad del Estado pueden facilitar a entidades bancarias adheridas a un Convenio, imágenes de atracos en sus sucursales** para conocer la forma de actuación de los delincuentes y prevenir la comisión de delitos.

De dicho informe se extrae lo siguiente:

El artículo 120 del Reglamento de la Ley de Seguridad Privada **impone especiales obligaciones en materia de videovigilancia a las entidades financieras de crédito**.

La Agencia ha analizado esta cuestión en diversas ocasiones **basándose en el efecto directo del artículo 7 f) de la Directiva 95/46/CE**, relativo **al interés legítimo** para el tratamiento de datos personales, y según éste, para que sea posible la comunicación de datos será necesario determinar en cada caso concreto **si la ponderación de los derechos e intereses de los perjudicados puede justificar o no dicho tratamiento de los datos** de carácter personal.

Dado que la finalidad de la comunicación de los datos en el caso concreto es prevenir futuros hechos ilícitos con peligro para las personas y bienes en las sedes de las entidades de crédito asociadas al Convenio, **podría considerarse criterio suficientemente relevante como para justificar el intercambio de información**.

Por tanto, **será lícita la cesión de imágenes grabadas** siempre que en el Convenio del que forman parte las entidades de crédito se inserten las medidas de seguridad establecidas por la LOPD y el Reglamento de Desarrollo sobre el acceso a las imágenes, las medidas en caso de incumplimiento de las normas de seguridad y el plazo de conservación de las imágenes.

IMPORTANTE

Los datos personales relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes.

ACTUALIDAD LOPD

La inserción indebida en ficheros de morosidad y la contratación irregular, principales reclamaciones planteadas ante la AEPD

Fuente: *www.agpd.es*

La inserción indebida en ficheros de morosidad y la contratación irregular, principales reclamaciones planteadas ante la AEPD

La Agencia ha publicado su Memoria correspondiente a 2015, donde se constata un incremento del 15,70% en el número de denuncias y reclamaciones resueltas. Los sectores más sancionados en 2015 han sido telecomunicaciones, entidades financieras, y suministro y comercialización de energía y agua.

- Las consultas planteadas ante la AEPD crecieron más de un 10% en 2015, superando las 218.000 cuestiones
- El derecho de cancelación se mantiene como el más ejercitado por los ciudadanos, que dan prioridad a que sus datos se eliminen cuando así lo solicitan

Madrid, 21 de junio de 2016. La Agencia Española de Protección de Datos (AEPD) ha publicado hoy su Memoria 2015, que recoge de manera exhaustiva la actividad y el funcionamiento de las distintas áreas de la institución, las tendencias más destacadas, las decisiones y procedimientos más relevantes del año y un completo análisis de los desafíos presentes y futuros en materia de protección de datos.

El **análisis de la actividad anual** refleja un incremento en el número de denuncias y reclamaciones resueltas. Así, en 2015 se han resuelto 10.871 denuncias frente a las 9.404 resueltas en 2014 (+15,60%). En cuanto a las reclamaciones de los ciudadanos para ejercer sus derechos de acceso, rectificación, cancelación y oposición (ARCO), se han resuelto 2.113 en 2015 frente a las 1.818 de 2014 (+16,23). De estos datos se desprende que ha habido un incremento medio en la resolución de reclamaciones y denuncias de un 15,70% respecto a 2014. En lo que respecta a denuncias y reclamaciones planteadas ante la AEPD por los ciudadanos en 2015, se han recibido un total 10.571, una cifra que supone una consolidación con respecto a años anteriores tras el repunte de 2014.

La **inserción indebida en ficheros de morosidad y la contratación irregular** se encuentran entre las principales reclamaciones planteadas ante la Agencia Española de Protección de Datos por los ciudadanos. Uno de cada tres afectados denunció ante la AEPD cuestiones relacionadas con el ámbito de la morosidad, en particular la inclusión en ficheros comunes, la reclamación de deudas impagadas o la contratación irregular en servicios ofrecidos por operadores de telecomunicaciones, entidades financieras o compañías energéticas. En relación con estas conductas es preciso incidir que la inclusión indebida en ficheros de morosidad produce unos efectos especialmente negativos para los afectados, por los que las empresas deben extremar su diligencia antes de comunicar una información inexacta.

Puede ver más información en el siguiente enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_06_20-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Qué he de hacer para cumplir con la Ley Orgánica de protección de Datos?

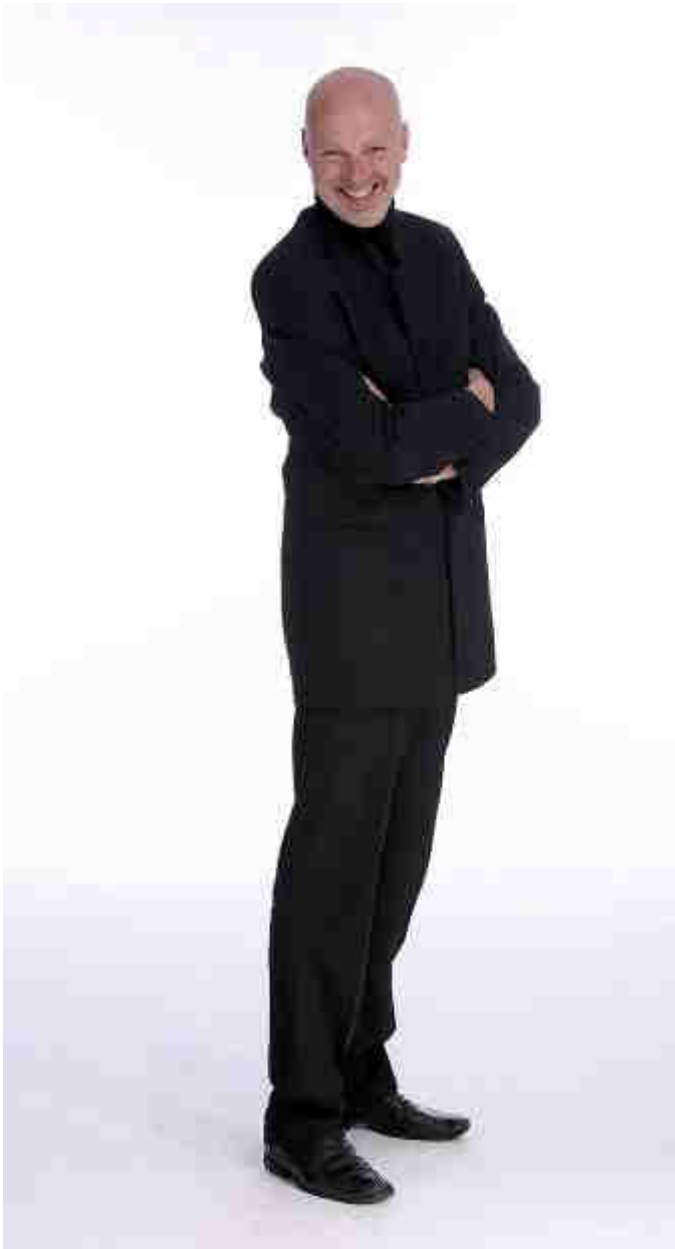
Una de las obligaciones del responsable del fichero es **proteger los datos personales** que trata en el desarrollo de su actividad.

Los riesgos a que están expuestos los ficheros pueden venir, tanto de la acción humana (trabajador despedido que se lleva la base de clientes), como de circunstancias naturales, o de accidentes fortuitos (inundación que destruye un equipo informático o la documentación en papel).

Resulta necesario que **el responsable del fichero adopte las medidas adecuadas y necesarias para garantizar la protección de datos de carácter personal** y evitar su destrucción, pérdida, alteración, difusión o acceso no autorizado.

A tal efecto, entre otras cosas, deberá:

- Determinar las funciones y obligaciones del personal con acceso a datos.
- Elaborar un Documento de Seguridad e implantar las medidas de seguridad.
- Llevar un registro de incidencias.
- Llevar un control de acceso a los recursos.
- Gestionar los soportes y documentos.
- Identificar y autenticar a los usuarios.
- Realizar copias de respaldo.
- Nombrar a un responsable de seguridad.
- Realizar una auditoría bienal.
- Llevar un control de acceso físico a equipos.
- Llevar un registro de accesos a datos sensibles.
- Gestionar el acceso a la documentación en papel.



IMPORTANTE

El responsable del fichero debe asegurarse de que las medidas de seguridad no sólo son conocidas en la organización, sino que efectivamente se aplican.