

LA LOPD EN EL DÍA A DÍA

Las cámaras de vigilancia y el cumplimiento de la LOPD

El cumplimiento de la LOPD en lo relativo a videovigilancia se desarrolla así:

1. INSCRIPCIÓN DE FICHEROS

Sólo si existe grabación de las imágenes se deberá notificar el fichero relativo a dichas imágenes.

La simple reproducción en circuito cerrado ó emisión de imágenes en tiempo real no se considera fichero.

2. DEBER DE INFORMAR

Para informar adecuadamente debe existir:

- Un cartel de ZONA VIDEOVIGILADA.
- Un impreso informando de la existencia de un tratamiento, finalidad y destinatarios de la información, el ejercicio de los derechos ARCO, la identidad y dirección del responsable del fichero.

La información del impreso podrá incorporarse al cartel anunciador si la misma es legible.

3. CONTRATO DE ENCARGADO DEL TRATAMIENTO

Si una empresa externa accede ó puede acceder a las imágenes, se deberá suscribir el correspondiente contrato de encargado del tratamiento.

4. MEDIDAS DE SEGURIDAD

Se deberá elaborar un Documento de Seguridad e implantar las medidas de seguridad requeridas por la LOPD.

Contenido

Las cámaras de vigilancia y el cumplimiento de la LOPD	1
Empresa de marketing no puede acreditar origen de datos	2
La información en la recogida	3
3ª sesión anual abierta de la AEPD	4
¿Cuándo debemos actualizar el Documento de Seguridad?	5



IMPORTANTE

Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos.

Es decir, no podemos tener una cámara de vigilancia tomando imágenes de toda la calle.

El plazo máximo de cancelación de las imágenes grabadas es de un mes desde su captación.

SANCIONES DE LA AEPD

Empresa de marketing no puede acreditar origen de datos

El procedimiento sancionador de la AEPD [PS/00285/2009](#), iniciado a instancias de una denuncia presentada por un particular a la entidad OFERDATA S.L. pone de manifiesto la **necesidad que tienen las empresas dedicadas a marketing y prospección comercial de poder acreditar el origen de los datos personales que tratan para el desempeño de su actividad.**

En este caso, el hecho es que la denunciante recibió una publicidad de EUROLINEA HOGAR, en la que constaba que los datos habían sido facilitados por OFERDATA S.L..

En contestación al requerimiento de la AEPD, la empresa OFERDATA S.L. alegó que los datos habían sido recogidos de fuentes accesibles al público (páginas blancas, páginas amarilla, QDQ, etc.).

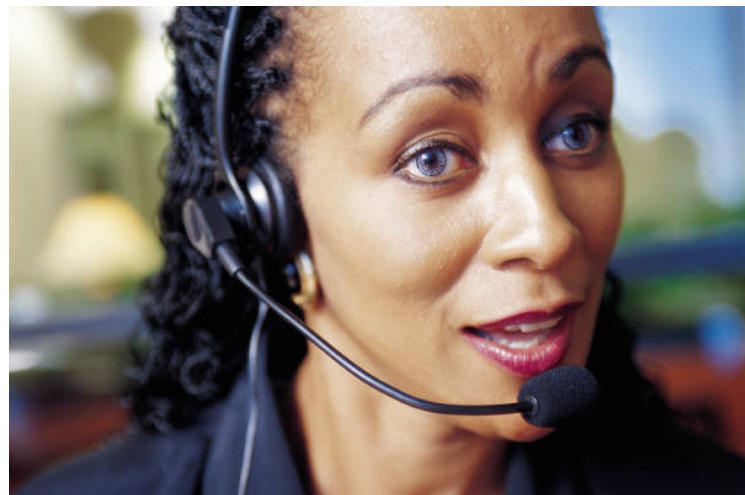
Sin embargo, el inspector de la AEPD no pudo encontrar en dichos repertorios el piso y puerta del denunciante, con lo que no se pueden entender obtenidos de dichas fuentes.

Al no ser los datos obtenidos de fuentes accesibles al público, es necesario probar que se ha obtenido el consentimiento de los titulares de dichos datos, cosa que OFERDATA S.L. no hizo.

Resultado: una sanción de 60.101,21€ por vulneración del artículo 6 de la LOPD.

En esta sanción la AEPD no ha aplicado el art. 45.5 para rebajar la cuantía de la sanción porque ha considerado que la entidad no ha demostrado celo ni diligencia en el tratamiento de los datos.

“La recogida de datos para actividades de publicidad y prospección comercial debe realizarse de forma sumamente escrupulosa.”



IMPORTANTE

El RD1720/2007 hace referencia expresa a las entidades dedicadas a publicidad y prospección comercial.

Estas entidades deben ser sumamente escrupulosas en la recogida y tratamiento de los datos personales.

El poder acreditar la procedencia de los datos y el consentimiento en los casos que sea necesario, les obligará a adecuar tanto sus políticas como sus procedimientos.

LA AEPD ACLARA

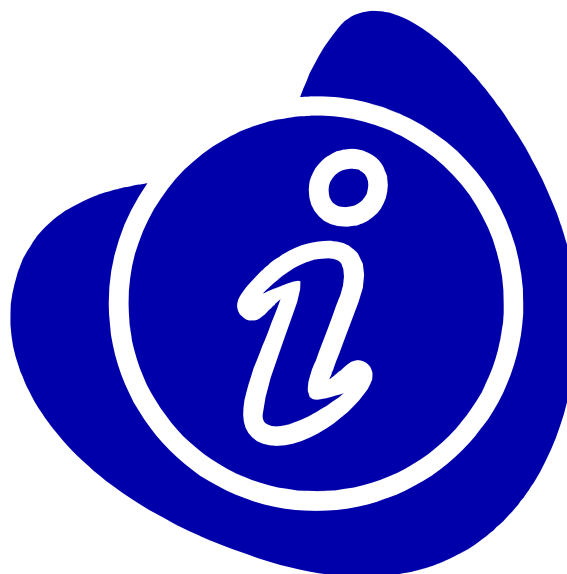
La información en la recogida

El informe [0340/2010](#) de la AEPD resuelve algunos interrogantes sobre cómo acreditar de que se ha informado adecuadamente a los titulares de los datos en la recogida de los mismos.

A tenor de dicho informe jurídico, será posible acreditar el derecho de información de las siguientes formas:

- **Recogida presencial:** documento firmado por el titular en el que conste que ha sido informado.
- **Recogida en web:** formulario en la web en el que sea imprescindible la aceptación de la cláusula informativa por parte del titular para poder efectuar el tratamiento de los datos.
- **Recogida telefónica:** a través del establecimiento de una alocución permanente grabada en la que se haga referencia al tratamiento de los datos informando de los extremos contenidos en el art. 5.1 de la LOPD y de la conservación de las cintas mientras dure el tratamiento de los datos.

Debe tenerse en cuenta, además, que la información debe ser siempre comprensible y adecuada a las personas con necesidades específicas (por ejemplo, niños y ancianos).



A TENER EN CUENTA

Antes de realizar la recogida de los datos personales, debemos pensar en **cómo podremos demostrar** que hemos informado a los titulares de esos datos.

Debemos también **reflexionar** sobre si la **información que aportamos** en la recogida **es comprensible** para el público al que vamos a recoger dichos datos.

ACTUALIDAD LOPD

3ª sesión anual abierta de la AEPD

Fuente: www.agpd.es

The image shows the cover of a guide titled '3ª SESIÓN ANUAL ABIERTA DE LA AEPD'. The cover features the AEPD logo and the Spanish coat of arms at the top left, and a graphic with the number '3' and the text '3ª Sesión Anual Abierta de la AEPD' at the top right. The main title is '3ª SESIÓN ANUAL ABIERTA DE LA AEPD', followed by the subtitle 'Guía sobre Protección de datos en las Administraciones Públicas y la Administración Electrónica'. Below the subtitle, the names of the authors are listed: 'Jesús Rubí Navarrete, Adjunto al Director' and 'Ricard Martínez Martínez, Coordinador del Área de Estudios'. At the bottom, it says 'Agencia Española de Protección de Datos' on the left and 'Madrid, 20 de octubre de 2010' on the right.

El día 20 de Octubre tuvo lugar la 3ª sesión anual de la Agencia Española de Protección de Datos.

En esta sesión se trataron temas como la administración electrónica y las principales novedades y desarrollos en materia de protección de datos personales.

También se contestaron numerosas consultas que habían hecho los asistentes vía web.

La AEPD destaca el papel esencial de la protección de datos en la implantación de la e-administración.

EL PROFESIONAL RESPONDE

¿Cuándo debemos actualizar el documento de seguridad?

Una consulta muy frecuente es la relativa a la actualización del documento de seguridad.

El artículo 88.7 del RD1720/2007 dice:

El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados.

Situaciones en las que debemos actualizar el documento de seguridad:

- **Se incorpora un nuevo trabajador que va a tratar datos personales a la empresa.** Deberá añadir a la lista de usuarios y accesos permitidos.
- **Se va de la empresa un trabajador que tenía acceso a datos personales.** Deberá eliminar de la lista de usuarios y accesos permitidos.
- **Se compra nuevo equipamiento informático.** Se deberá añadir al inventario de equipamiento de la sede en la que se produzca la adquisición.
- **Se adquiere un nuevo software.** Se deberá añadir el software en su sección así como los perfiles que tienen acceso a mismo.
- **Se recogen nuevos tipos de datos.** Se deberá modificar la inscripción

“Hay que estar pendiente de los cambios y reflejarlos en el Documento de Seguridad.”



del fichero y el documento de seguridad para describirlo.

- **Se incorpora o cambia algún encargado del tratamiento.** Se deberá suscribir el correspondiente contrato y modificar, además, la inscripción del fichero si es caso.
- **Cuando se produzcan otros cambios en la organización.**