Boletín 01/14

LOPD EN LA EMPRESA

Aselio | PROTECCIÓN DE DATOS

LA LOPD EN EL DÍA A DÍA

¿Qué autorizaciones deben estar documentadas?

El cumplimiento del RD1720/2007 requiere que tengamos en el Documento de Seguridad una relación de las personas y/o perfiles a los que se ha concedido alguna autorización:

- Lista de usuarios que pueden **sacar datos personales fuera** de las instalaciones del responsable del fichero (N. Básico).
- Lista de usuarios que pueden **tratar datos personales fuera** de las instalaciones del responsable (N. Básico).
- Lista de usuarios que pueden **tratar datos** personales en **dispositivos portátiles** (N. Básico).
- Lista de usuarios que tienen **acceso a los dispositivos** (armarios, cajoneras, etc.) donde se **almacenan los soportes** que contienen datos personales (N. Básico).
- Lista de usuarios que tienen **acceso a los locales** donde **están los sistemas** de información (equipos) que tratan los ficheros (N. Medio).
- Lista de usuarios autorizados para **enviar y/o recepcionar soportes** automatizados que contienen datos personales (N. Medio).
- Lista de usuarios autorizados para **copiar documentos** que **contienen datos** personales de nivel alto (N. Alto).

Contenido

IMPORTANTE

Estas listas de usuarios autorizados deben mantenerse en todo momento actualizadas, reflejando la realidad de la organización.

SANCIONES DE LA AEPD

Denuncia de oficio relacionada con la videovigilancia

En el procedimiento sancionador PS/00327/2010 de la AEPD podemos ver cómo la propia **POLICIA MUNICIPAL DE MADRID denuncia la instalación** de un sistema de videovigilancia que no cumple los requisitos que marca la normativa sobre protección de datos personales.

Las instalaciones de videovigilancia son las que más denuncias provocan ante la AEPD.

Según los hechos, la policía municipal de Madrid denuncia ante la Agencia Española de Protección de Datos la instalación de cámaras de videovigilancia en el establecimiento "La Cervesía", titularidad de XXX, S.L. sin cumplir los requisitos exigidos por la LOPD.

Los inspectores de la AEPD constatan que en dicho establecimiento **no existen los carteles informativos de videovigilancia** donde se informa a los afectados de la existencia de dicho tratamiento, así como de la identidad del responsable del mismo y dónde pueden ejercer sus derechos de acceso y cancelación.

En este caso la entidad denunciada ha **recabado datos personales (las imágenes grabadas) sin facilitar a sus titulares la información** que señala el artículo 5 de la LOPD por lo que debe considerarse que ha incurrido en una infracción leve al no facilitar dicha información de forma visible.

Resultado: Teniendo en cuenta los criterios de graduación de las sanciones previstos en el citado artículo 45.4 de la LOPD y, en especial, la falta de beneficios obtenidos y al grado de intencionalidad, la AEPD procede a sancionar al establecimiento con una multa de 2.000€.

IMPORTANTE

La denunciante es la propia **policía municipal**, que ha puesto el caso en manos de la AEPD **actuando "de oficio"** al detectar que una instalación de **videovigilancia** no estaba de acuerdo a la LOPD.

LA AEPD ACLARA

El informe de auditoría y su conservación

El informe 0191/2010 de la AEPD aclara el plazo de conservación de los informes de auditoría que exige la LOPD para los ficheros de nivel medio y alto.

De dicho informe jurídico se extrae lo siguiente:

- **A partir de nivel medio,** los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos **cada dos años, a una auditoría** interna o externa.

- Con **carácter extraordinario** deberá realizarse dicha auditoría siempre que se **realicen modificaciones sustanciales** en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. **Esta auditoría inicia el cómputo de dos años** señalado en el párrafo anterior.

- Teniendo en cuenta los plazos de prescripción y de **obligación** de sometimiento a la auditoría, el término durante el cual el **informe debería estar a disposición** de la Agencia Española de Protección de Datos o autoridad autonómica de control competente debería ser el de **dos años**.

- Solo existe la obligación de guardar el **último informe de auditoría**.

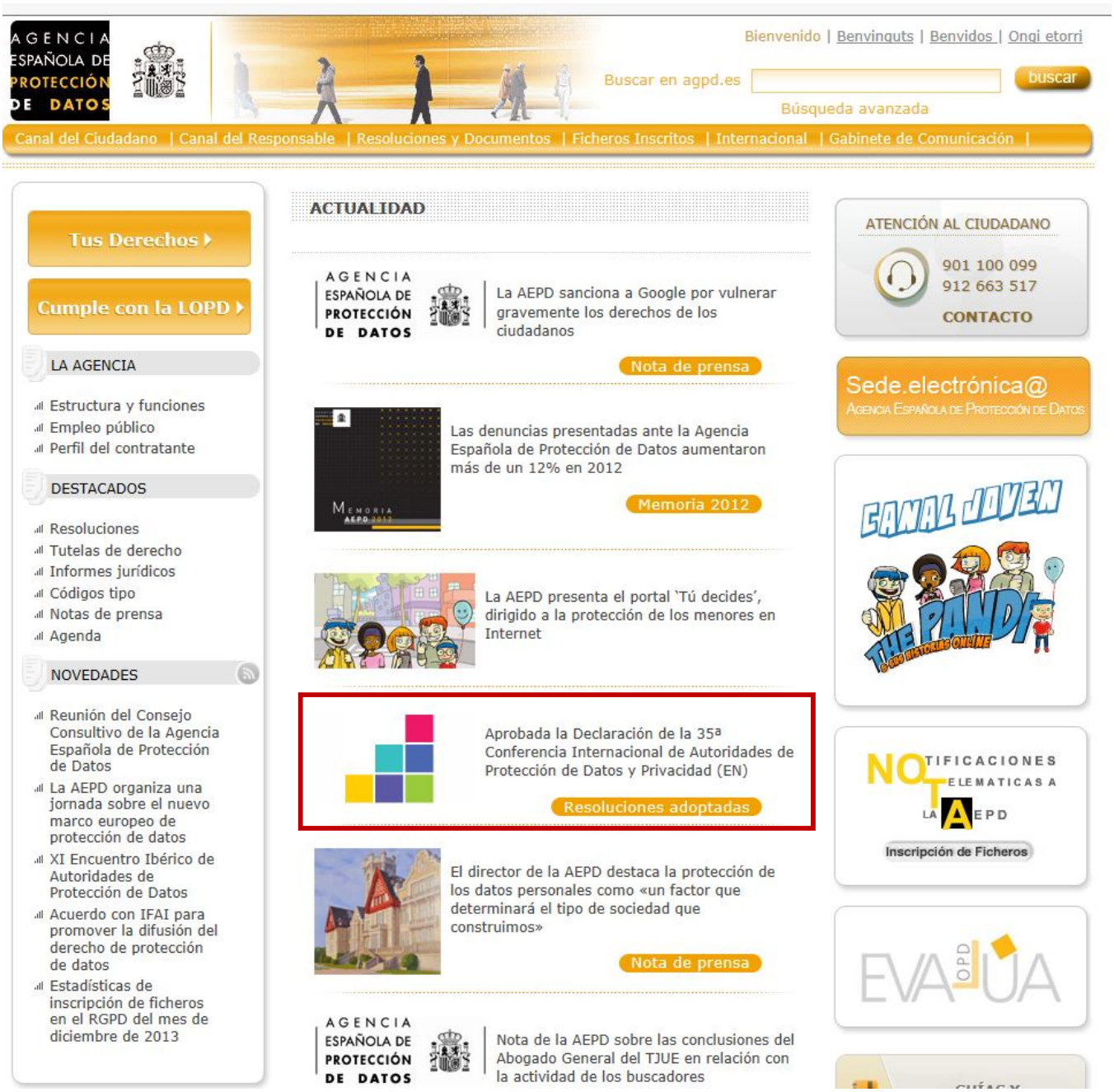
IMPORTANTE

No realizar la obligada auditoría en los plazos que marca la Ley es una infracción grave, con sanción de entre 40.001 y 300.000€.

ACTUALIDAD LOPD

Aprobada la Declaración de la 35ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (EN)

Fuente: www.agpd.es



Puede ver más información en el siguiente enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/octubre/130924_Warsaw_declaration.pdf

EL PROFESIONAL RESPONDE

¿Cómo puedo limitar el acceso a los equipos?

Una pregunta que hacen muchos clientes es: de qué forma puedo limitar el acceso a los equipos, de forma que los usuarios únicamente accedan a los recursos necesarios para su trabajo.

Existen diversas maneras de identificación y autenticación del usuario en función del mecanismo o tecnología que se aplique.

Podemos clasificar los sistemas en estos tipos:

- Sistemas basados en algo que el usuario **conoce** (contraseña).
- Sistemas basados en algo que el usuario **posee** (DNI electrónico, token, etc.).
- Sistemas basados en una característica **física** del usuario, también denominados biométricos (reconocimiento de huella dactilar, voz, rostro, patrón ocular, etc.).
- Sistemas **mixtos**, que combinan dos o más de los descritos anteriormente.

En caso de que utilicemos el sistema más extendido, a través de contraseñas, para garantizar la seguridad se debe realizar una correcta gestión de las mismas:

- Evitar todas aquellas contraseñas deducibles por terceros y asociadas a parámetros comunes del usuario (fechas de nacimiento, nombre de familiares, matrículas de coches, aficiones, etc.).
- Emplear al menos 6 caracteres combinando mayúsculas, minúsculas, números y otros caracteres especiales.
- Establecer la periodicidad de cambio de las contraseñas a menos de 1 año.
- Limitar el número de intentos fallidos de acceso al sistema.

"Como Responsables de Fichero, debemos implantar mecanismos para limitar el acceso a los sistemas de información"

A TENER EN CUENTA

No tener implantadas las medidas de seguridad es una infracción grave, con sanción de entre 40.001 y 300.000€.