Boletín 09/13

LOPD EN LA EMPRESA

Aselio | PROTECCIÓN DE DATOS

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

LA LOPD EN EL DÍA A DÍA

Recogida de datos personales del propio interesado

El **momento más importante** para el correcto cumplimiento de la normativa de protección de datos es, sin duda, el momento de la **recogida de los datos**.

Es en ese momento cuando debemos informar de la **finalidad** para la cual se recaban dichos datos (por ejemplo, elaborar la factura solicitada), la **identidad y domicilio del responsable del fichero** y dónde pueden ejercerse los derechos de acceso, rectificación, cancelación y oposición.

En el caso de que se vaya a producir una **cesión de los datos** (como por ejemplo, una agencia de viajes que ceda posteriormente datos al tour-operador), se deberá informar al titular de los datos, además, de la **finalidad de dicha cesión y el sector** al que pertenece el **destinatario** de la misma (puede ser necesario, además, solicitar el consentimiento para la misma si no está amparada dicha cesión en alguna de las excepciones previstas por la Ley).

Para cumplir correctamente con este principio de información, es necesario **adecuar los formularios** que utilice la empresa para recoger dichos datos **añadiendo la cláusula informativa** correspondiente (es recomendable añadirla también en facturas, presupuestos, etc.).

Entre los formularios que se deben adecuar a la LOPD, no debemos olvidar el **formulario de contacto de la página web. Página que debe estar adecuada también a la LSSICE**.

Contenido

A TENER EN CUENTA

Corresponde a la entidad demostrar que ha informado de forma adecuada a la persona que ha suministrado sus datos.

SANCIONES DE LA AEPD

Sanción colocar pantallas de videovigilancia al público

En la resolución R/01776/2013 de la AEPD se puede ver la **sanción que puede sufrir una empresa por tener colocados los monitores de las cámaras de videovigilancia al público, así como no tener legalizadas dichas cámaras conforme la LOPD.**

La carga de la prueba corresponde siempre a la entidad.

El establecimiento fue denunciado por el Puesto de Palamós de la Guardia Civil.

El Director de la AEPD resolvió requerir al denunciado para que **regularizase**, en el plazo de **un mes**, la **situación de su sistema de videovigilancia** y acreditase la realización de las siguientes acciones:

- **Retirar las pantallas** en las que se visualizan imágenes captadas, de forma que no sean visualizadas por todo el público que accede, sino solo por el responsable del fichero.
- **Exponer** en su establecimiento **carteles informando de la presencia de cámaras** y en los que se especifique la entidad ante la cual ejercer los derechos de acceso, rectificación, cancelación y oposición.
- **Inscribir el fichero** con la finalidad "videovigilancia".

Sin embargo, finalizado el plazo acordado, el denunciado no había adoptado todas las medidas correctoras solicitadas, iniciándose el procedimiento sancionador.

En el transcurso del procedimiento sancionador la entidad denunciada aportó fotografías en la que hacía constar la ausencia de las pantallas y la colocación de los carteles informativos, así como el certificado de inscripción del fichero**.**

Resultado: Sanción de 1.000 € por infracción del artículo 37.1.a) de la LOPD.

IMPORTANTE

El cartel de videovigilancia, para que sea válido, debe indicar la entidad o persona y el domicilio ante el que se ejercen los derechos de acceso, rectificación, cancelación y oposición.

LA AEPD ACLARA

Medidas de seguridad a adoptar por asesor

El informe jurídico 0524/2009 de la AEPD resuelve la consulta planteada, sobre **diversas cuestiones relativas al nivel de seguridad que habrá de implantarse sobre los ficheros relacionados con la actividad de asesoramiento fiscal**, desarrollada por el consultante. En particular se consulta si los datos relativos a la asignación a la Iglesia Católica, donaciones deducibles efectuadas a ONG, grado de discapacidad, importe de la cuota sindical y matrimonio entre personas del mismo sexo, constituyen datos especialmente protegidos que exijan la adopción de medidas de seguridad de nivel alto.

De dicho informe jurídico se extrae lo siguiente:

- El dato relacionado con la **asignación de la Iglesia Católica** no revela, necesariamente, las creencias religiosas de una persona.
- El dato relativo a la **discapacidad**, siempre que se trate **con motivo del cumplimiento de deberes públicos opera la excepción** prevista en el art. 81.6 del Reglamento y es posible la implantación de medidas de seguridad de **nivel básico**.
- El dato relativo a la **cuota sindical**, siempre que se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan datos especialmente protegidos sin guardar relación son su finalidad, **opera la excepción prevista en el art. 81.5.b)** del Reglamento y podrán implementarse medidas de seguridad de **nivel básico** (aquí el informe recoge que "siempre que sea en formato papel", sin embargo, la disposición adicional cuarta del R.D. 3/2010 cambó la redacción del art. 81.5b) del Reglamento). Esta excepción resulta aplicable también a los supuestos de **deducciones por donaciones**.
- Respecto a la constancia en la declaración de la renta de **matrimonio entre personas del mismo sexo**, éste **no es un dato especialmente protegido**.

A TENER EN CUENTA

Los datos recogidos deben ser adecuados, pertinentes y no excesivos para la finalidad a la que van a ser destinados.

ACTUALIDAD LOPD

El próximo 15 de octubre concluye el plazo para presentar las candidaturas a los "Premios Protección de Datos 2013"

Fuente: www.agpd.es

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Nota informativa

Este año se celebra la XVII edición

El próximo 15 de octubre concluye el plazo para presentar las candidaturas a los "Premios Protección de Datos 2013"

- **Los galardones, que se convocan en las categorías de 'Comunicación' e 'Investigación', reconocen aquellos trabajos que supongan una aportación destacada a la difusión de este derecho fundamental**
- **Los premios y accésits de cada categoría cuentan con una dotación económica de 3.000 y 1.500 euros respectivamente**

(Madrid, 17 de septiembre de 2013). El próximo 15 de octubre finaliza el plazo para presentar las candidaturas a la XVII edición de los Premios Protección de Datos Personales en las categorías de **'Comunicación' e 'Investigación'**, que convoca la Agencia Española de Protección de Datos (AEPD).

El **PREMIO PROTECCIÓN DE DATOS PERSONALES DE COMUNICACIÓN 2013**, dotado con 3.000 euros, así como un accésit de 1.500 euros, tiene por objeto reconocer los **trabajos de medios y profesionales de la comunicación** que supongan una aportación destacada a la promoción de este derecho fundamental y hayan contribuido a fomentar la concienciación tanto de los ciudadanos como de las entidades que manejan información personal.

Podrán optar a este premio tanto trabajos individuales -como un editorial, noticia, reportaje, o programa de radio o televisión- puntualmente dedicados a la materia objeto de la convocatoria, como proyectos periodísticos -tales como series de noticias o secciones especializadas- que definan un compromiso editorial con la promoción del derecho fundamental a la protección de datos. Es requisito para optar al premio que los trabajos hayan sido difundidos entre el 16 de octubre de 2012 y el 15 de octubre de 2013.

Puede acceder desde este enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/septiembre/130917_NP_Recordatorio_Premios_2013.pdf

EL PROFESIONAL RESPONDE

La copia de seguridad, ¿cada cuánto tiempo debe hacerse?

Independientemente del nivel de seguridad de los ficheros, se debe realizar una **copia de respaldo al menos una vez a la semana,** que permita restablecer los ficheros al momento anterior al producirse la pérdida.

Obviamente, si no se han modificado datos de los ficheros esa semana, no es necesario realizar la copia de seguridad, ya que con la anterior será suficiente.

De los **ficheros de nivel alto**, además de realizarse la copia de seguridad semanal debe **existir otra copia fuera de las instalaciones principales**, de forma que si ocurre una catástrofe (incendio, inundación, etc.) no se pierdan todos los datos, y podamos recuperarlos de la copia remota.

En este aspecto, debemos tener en cuenta que dicha **copia remota deberá estar cifrada**, de forma que sólo puedan acceder a la información contenida en la misma las personas autorizadas para ello.

De cara a la recuperación de los datos debemos tener en cuenta lo siguiente:

1. Debemos anotar en el **registro de incidencias** dicha pérdida de datos y su recuperación posterior.
2. En el caso de que sean copias de respaldo de **ficheros de nivel medio o alto**, deberá ser **autorizada por el responsable del fichero** y en el registro de incidencias deberán consignarse, además, los procedimientos realizados de recuperación de los datos, **indicando la persona que ejecutó el proceso**, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

A TENER EN CUENTA

No tener implantadas las medidas de seguridad que establece la normativa es una infracción grave, sancionada con multa de entre 40.001 € y 300.000 €.