Boletín 04/14

LOPD EN LA EMPRESA

Balaguer & Gutiérrez
Correduría de Seguros
Consultoría de Protección de Datos

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

LA LOPD EN EL DÍA A DÍA

¿Qué es una persona identificada o identificable?

Un dato de carácter personal es **cualquier información** numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo **concerniente a personas físicas identificadas o identificables**.

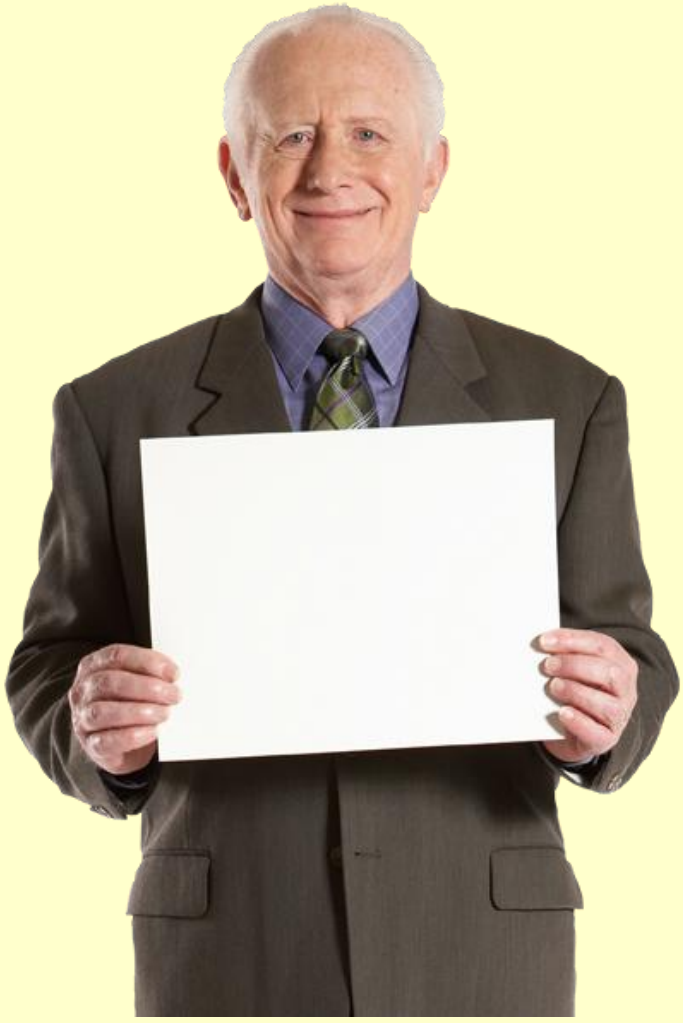
Los datos personales, permiten pues, identificar a una persona, así como revelar información de la misma.

Persona identificada: toda persona cuya **identidad está determinada**.

Persona identificable: toda persona cuya **identidad pueda determinarse**, ya sea directamente o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

Vamos a matizar el concepto de identificable. Si recabamos imágenes a través de una cámara de vigilancia, las imágenes recogidas, pertenecen a personas, que podemos, o no, identificar. Si las **imágenes se captan con una resolución tal que permitan identificar a una persona, ésta sería una persona identificable**, y estaría dentro del ámbito de la ley, en caso contrario, no.

Contenido



IMPORTANTE

Se debe realizar un análisis dentro de la empresa de los datos que se tratan para poder asignar correctamente el nivel de medidas de seguridad a aplicar.

SANCIONES DE LA AEPD

Sanción por carecer de medidas de seguridad

En la resolución R/01306 de la AEPD podemos ver la **sanción** que puede sufrir una entidad **por no tener implantadas las medidas de seguridad exigidas.**

Las medidas de seguridad, además de figurar en el documento de seguridad, han de implantarse

Con fecha 29 de marzo de 2010 tiene entrada en la AEPD un escrito de D. A.A.A., en el que declara que, la empresa HIPERCOR, S.A., **no cuenta con las medidas de seguridad oportunas con relación a información de datos clínicos**, ya que desde dos terminales ubicados en el muelle de recepción de mercancías, donde tiene su puesto de trabajo, se pueden visualizar, entre otros, análisis clínicos de trabajadores de la empresa.

Durante la visita de las inspectoras de la AEPD, el denunciante accede a un equipo informático que está en el muelle, observándose que **aunque el sistema pide un usuario y contraseña para acceder, el usuario sale ya por defecto, y la contraseña es la misma que el nombre de usuario**.

Se puede además comprobar que desde ese equipo, a través de la red local **es posible acceder a carpetas que están situadas en el equipo de la Jefa de Recursos Humanos** del centro, en concreto es posible acceder a una carpeta denominada "Servicio Médico" y que contiene los **resultados analíticos** de los empleados del centro.

A las 15:30 horas, las inspectoras de la Agencia y los representantes de la entidad, se trasladan al muelle, verificándose que ha sido subsanado el error.

Resultado: Sanción de 20.000 € por vulneración del artículo 9.1 de la LOPD en relación a las medidas de seguridad.

IMPORTANTE

El asesoramiento de un profesional en la aplicación de las medidas de seguridad es sumamente importante para una correcta implantación.

LA AEPD ACLARA

Tratamiento de datos de menores de edad

El informe 0046 de la AEPD resuelve la consulta planteada sobre **el tratamiento de datos personales de los menores de edad a los que se facilita una tarjeta de fidelización**.

De dicho informe jurídico se extrae lo siguiente:

a) Si es un **menor de 14 años** ó incapaz, el **consentimiento** ha de ser **otorgado por los padres**.

b) La **cláusula informativa** debe estar elaborada en un **lenguaje comprensible a la edad** del menor.

c) **No se podrán recabar del menor datos que permitan obtener información sobre los demás miembros del grupo familiar**, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos, o cualesquiera otros, sin el consentimiento de los titulares de tales datos (únicamente podrán recabarse los datos de la identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado a).

d) **Corresponde al responsable del fichero articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento** prestado en su caso, por los padres, tutores o representantes legales.

IMPORTANTE

Hay que extremar las cautelas cuando se recogen datos de menores, en especial la obtención del consentimiento.

ACTUALIDAD LOPD

La AEPD amplía en marzo su sistema de notificación de quiebras de seguridad para proveedores de servicios de comunicaciones

Fuente: www.agpd.es

Nota de prensa

La Sede Electrónica alberga desde hoy el nuevo procedimiento

La AEPD amplía su sistema de notificación de quiebras de seguridad

- **Los proveedores de servicios de comunicaciones electrónicas están obligados a notificar a la Agencia las quiebras de seguridad que se produzcan en sus sistemas y que puedan afectar a los datos personales que tratan**
- **La AEPD ha puesto en marcha un sistema de notificación rápido y seguro que está disponible a través del apartado 'Notificación preceptiva de quiebras de seguridad' de la Sede Electrónica de la Agencia**
- **El Reglamento de la Comisión Europea 611/2013, que recoge esta y otras obligaciones, tiene como objetivo reforzar las garantías de los abonados o particulares ante la destrucción, pérdida, alteración, revelación o acceso no autorizado a sus datos personales**

(Madrid, 23 de marzo de 2014). La Agencia Española de Protección de Datos (AEPD) ha puesto en marcha un nuevo sistema para que los proveedores de servicios de comunicaciones electrónicas notifiquen las eventuales quiebras de seguridad que se hayan producido en sus sistemas y que puedan afectar a los datos personales que tratan.

La Directiva 2002/58/CE establece que los proveedores de servicios de comunicaciones electrónicas disponibles para el público **están obligados a notificar las quiebras de**

Puede ver más información en el siguiente enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/abr_14/140423_NP_Notificacion_quiebras.pdf

EL PROFESIONAL RESPONDE

¿Qué se debe hacer, de cara al cumplimiento de la LOPD, cuando un trabajador se va de la empresa?

Para cumplir correctamente la LOPD, cuando se va un trabajador a la entidad, debemos realizar las siguientes acciones:

1. **Eliminar o marcar la fecha de baja de este usuario en la lista de usuarios y accesos autorizados**, de forma que ya no conste en el documento de seguridad como usuario autorizado para acceder a los ficheros con datos personales.

2. **Eliminar o bloquear el identificador que tenía asignado** para el acceso a los sistemas.

3. **Dar de baja las autorizaciones que tuviera** ese trabajador para sus funciones:

    a. Salida de soportes y/o documentos fuera de las instalaciones.

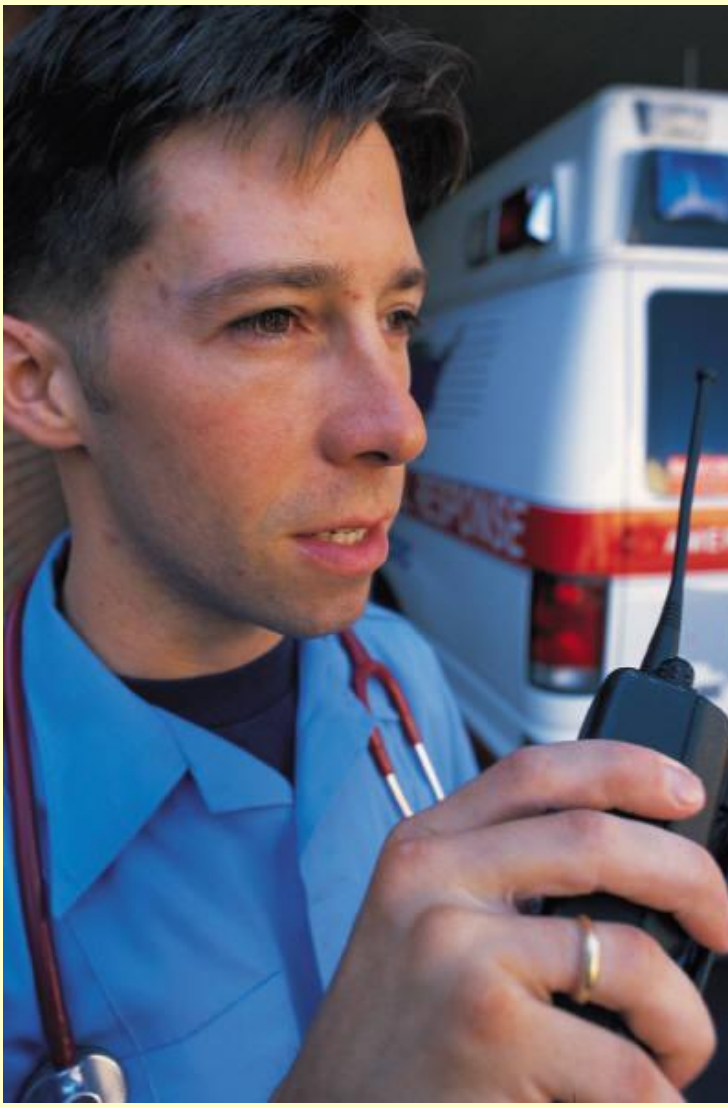
    b. Uso de portátiles.

    c. Trabajo fuera de los locales.

    d. Dispositivos a los que tiene acceso.

    e. Etc.

4. **Cancelar** todos los **privilegios** de ese trabajador así como las **conexiones remotas** que tuviera habilitadas.



IMPORTANTE

Hay que establecer protocolos de actuación que contemplen las acciones a realizar cuando un trabajador abandona la entidad.