Boletín 12/20

LOPD EN LA EMPRESA

Autor: Julio César Miguel Pérez

Balaguer & Gutiérrez
Correduría de Seguros
Consultoría de Protección de Datos

EL RGPD UE 2016/679 EN APLICACIÓN

El tratamiento de los sistemas de denuncias internas

En el art.24 de la LOPDGDD encontramos la referencia a este tratamiento. **A través de estos sistemas de información de denuncias internas se podrá poner en conocimiento de una entidad, incluso de forma anónima, la comisión de actos que sean contrarios a la normativa general o sectorial**, con independencia de que se hayan producido en la misma entidad o bien por terceros contratados por ella.

Los requisitos a tener en cuenta para su creación y mantenimiento:

1º Informar a los empleados y terceros.

2º Acceso exclusivo por el personal que desarrolle funciones de control interno y de cumplimiento.

3º Aplicar medidas para preservar la identidad y garantizar la confidencialidad de las personas afectadas por la información suministrada.

4º Suprimir los datos transcurridos tres meses desde la introducción de los datos.

5º Podrán conservarse en el sistema de forma anonimizada aquellas denuncias a las que no se hayan dado curso.

Los datos de las denuncias sobre las que existe una investigación de los hechos se podrán seguir tratando una vez transcurridos los tres meses, aunque no se incluirán en el sistema de denuncias internas.

Contenido

IMPORTANTE

Será licita su comunicación a terceros cuando sea necesaria para la adopción de medidas disciplinarias.

SANCIONES DE LA AEPD

Sancionado un autónomo por incumplir los requisitos legales en su página web

En el procedimiento sancionador https://www.aepd.es/es/documento/ps-00185-2020.pdf se sanciona a un autónomo con una multa de 3.000 euros por incumplimiento de su página web.

La AEPD es una de las autoridades que más sanciones impone en la U.E.

La reclamante presenta una denuncia ante la AEPD puesto que en la página web, a través de la cual se pueden adquirir juegos de placa de matrícula, es necesario facilitar datos personales tales como, nombre y apellidos, DNI, matrícula del vehículo y nº de bastidor no existían medidas de seguridad ya que se accedía sin protocolo de seguridad "htpp" y tampoco había ninguna política de privacidad. La reclamante intentó ponerse en contacto con el titular de la web sin conseguirlo.

La AEPD en el proceso de investigación constató las siguientes deficiencias:

1º Protocolo de seguridad; Sanción1.000 euros. Incumplimiento art. 32 RGPD. El acceso a la página se hacía con protocolo "http", lo que facilitaba que otros usuarios pudieran interceptar la información.

2º Política de privacidad; Sanción 1.000 euros. Incumplimiento art. 13 RGPD. La página hacía referencia a la antigua normativa *(Ley 15/1999 de Protección de datos de carácter personal)*.

3º Política de cookies; Sanción 1.000 euros. Incumplimiento art.22.2 LSSI. No existe banner informativo de primera capa ni mecanismo que permita rechazarlas en la segunda capa informativa.

IMPORTANTE

Existe una creciente concienciación por parte de los usuarios de los servicios de información por saber cómo se recogen sus datos personales.

LA AEPD ACLARA

Instalación de un sistema de videovigilancia que capta la imagen y voz de las personas que acceden al edificio

El Gabinete Jurídico de la APED https://www.aepd.es/sites/default/files/2019-09/informe-juridico-rgpd-grabacion-de-imagenes-y-voz-proporcionalidad.pdf responde con este informe a la duda planteada por un Ayuntamiento sobre la licitud de incorporar un sistema de videovigilancia con fines de "Seguridad y control de acceso a edificios" "y control de presencia de empleados" que grabase las imágenes y la voz.

En este sentido hay que considerar que tanto la imagen como la voz de la persona es un dato personal y por lo tanto supone un tratamiento que debe protegerse conforme a la normativa de protección de datos.

En relación con la instalación de sistemas de videocámaras deberá respetar el principio de proporcionalidad, valorando así, adoptar medios menos intrusivos, y que sea ponderada derivándose más beneficios que perjuicios para el interés general. Aplicando, además, el principio de minimización de datos de forma que estos sean adecuados pertinentes y limitados en relación con los fines para los que son tratados.

El Gabinete Jurídico indica en el informe que la legitimación de la videovigilancia por razones de seguridad no implica necesariamente la legitimación de la grabación de la voz, puesto que las grabaciones indiscriminadas de voz y conversaciones de los empleados y público en general que accede al edificio resultarían incompatibles con el principio de proporcionalidad.

IMPORTANTE

La omisión del cartel informativo de los sistemas de videovigilancia supone una infracción penalizada en la LOPDGDD

ACTUALIDAD LOPD

La AEPD publica una guía que analiza el uso de nuevas tecnologías en las Administraciones Públicas

Fuente: AEPD

(Madrid, 19 de noviembre de 2020). La Agencia Española de Protección de Datos (AEPD) ha publicado la Guía Tecnologías y Protección de Datos en Administraciones Públicas, en la que analiza algunas de las tecnologías que están aplicándose en las AAPP, los riesgos inherentes a su uso en lo relativo a la protección de datos personales y las salvaguardas que deben ser implementadas por estas. La Guía examina cookies y otras tecnologías de seguimiento, uso de las redes sociales, cloud computing, big data, inteligencia artificial, blockchain y smart cities. Su contenido se ampliará en versiones sucesivas, extendiéndolo a otras tecnologías específicas.

Los servicios implementados en las AAPP están guiados por el servicio público, si bien el tratamiento de datos personales que realizan tiene un riesgo característico derivado de la cantidad de datos recogidos, el volumen de personas afectadas, la imposibilidad de oponerse al tratamiento en muchos casos y el desequilibrio existente entre Administración y ciudadanos. Las AAPP, como responsables del tratamiento de los datos de los ciudadanos, antes de poner en marcha nuevas actividades de tratamiento o modificar servicios ya prestados, deben identificar los riesgos a los que puede estar expuesto el tratamiento y adoptar las medidas técnicas y organizativas que permitan eliminar o al menos mitigar los daños que pudieran derivarse del mismo para los derechos y libertades de las personas.

En cuanto al cloud computing, con sus indudables ventajas, presenta riesgos como la privacidad de la información almacenada, la continuidad de los servicios, los cambios legales y la pérdida de control de la infraestructura y las aplicaciones utilizadas. En el caso de las AAPP, por el volumen y la sensibilidad de los datos que gestionan, estos riesgos deben ser objeto de un riguroso análisis. No es improbable que en los servicios en la nube se produzcan brechas de seguridad que pongan en peligro la disponibilidad, la integridad o la confidencialidad de los datos personales, con consecuencias para los derechos y libertades de las personas físicas. Un ciberataque, un mal funcionamiento del sistema o un error humano pueden poner en peligro los datos de los ciudadanos. La gestión del riesgo de seguridad de la información no recae de forma exclusiva en la empresa proveedora del servicio que actúa como encargada de tratamiento, sino que corresponde a la Administración determinar las medidas de seguridad que debe de exigir al encargado y que, obligatoriamente, han de quedar reflejadas de forma contractual.

Puede ver más información en el siguiente enlace

Guía Tecnologías y Protección de Datos en Administraciones Públicas

EL PROFESIONAL RESPONDE

¿Cómo debe ser la participación del delegado de protección de datos en una entidad?

La figura del delegado de protección de datos (DPD) se está convirtiendo en relevante para muchas entidades, ya que les aporta seguridad y garantía del cumplimento de la normativa.

Para que el DPD pueda realizar sus funciones con éxito, el responsable y encargado del tratamiento tienen que garantizar los siguientes aspectos recogidos en el art.38 del RGPD;

1º Participar de forma adecuada y oportuna en las cuestiones relativas a la protección de datos personales. En este sentido, el Comité Europeo de protección de datos aconseja que, se invite al DPD a participar con regularidad en las reuniones con los cuadros directivos altos y medios.

2º Respaldar al DPD en todas sus funciones facilitando los recursos necesarios para su desempeño. Así como el acceso a los datos personales y operaciones de tratamiento.

3º Garantizar la independencia del DPD. No podrá recibir ninguna instrucción en lo que respecta al desempeño de sus funciones. Siguiendo con las recomendaciones del Comité Europeo, la opinión del DPD deberá tenerse siempre debidamente en cuenta, para ello, en caso de desacuerdo, sería conveniente documentar los motivos por los que no se sigue el consejo del DPD.

4º Evitar el conflicto de intereses con otras funciones desempeñadas por el DPD.

IMPORTANTE

El responsable y encargado del tratamiento no podrán oponer la existencia del deber de confidencialidad ante el acceso del DPD a los datos personales.