Boletín 01/21

LOPD EN LA EMPRESA

Balaguer & Gutiérrez
Correduría de Seguros
Consultoría de Protección de Datos

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

EL RGPD UE 2016/679 EN APLICACIÓN

Seguridad en el tratamiento y las brechas de seguridad

El responsable y encargado del tratamiento están obligados por la norma, así lo dice el art. 32 del RGPD, a garantizar un nivel de seguridad adecuados para evitar en la medida de lo posible las brechas de seguridad que supongan un riesgo para los datos personales tratados por ellos.

En este sentido, es importante que se lleve a cabo un análisis de riesgos que permita analizar el nivel de seguridad y la determinación de cuáles son las medidas técnicas y organizativas adecuadas, para que, en el caso de que se produzca una brecha de seguridad, el responsable y/o encargado del tratamiento sean capaces de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

¿A qué tipo de brechas de seguridad de datos personales tenemos que hacer frente?

- Brecha de confidencialidad: en aquellos casos en que no se tiene autorización para acceder a la información. La gravedad depende del alcance de la divulgación.
- Brecha de integridad: se modifica la información original y se sustituye por otra causando un perjuicio al afectado.
- Brecha de disponibilidad: no se puede acceder los datos originales cuando sea necesario.

Contenido

IMPORTANTE

Han aumentado las resoluciones sancionadoras de la AEPD en lo que se refiere al cumplimiento de las medidas de seguridad.

SANCIONES DE LA AEPD

Comercio online sancionado por no aplicar medidas de seguridad para garantizar la confidencialidad de los datos

En el procedimiento sancionador https://www.aepd.es/es/documento/ps-00185-2020.pdf se sanciona a un comercio online al no garantizar la confidencialidad de los datos personales de los clientes.

Los responsables, encargados del tratamiento y todas las personas que intervengan en el tratamiento están sujetas al deber de confidencialidad.

Los hechos reclamados tienen lugar cuando una usuaria del comercio reclamado accede a su cuenta y los datos personales que le aparecen no son los suyos sino los de otros clientes. Al ponerse en contacto con el comercio no obtiene respuesta, por lo que presentó una reclamación ante la AEPD.

En el proceso de investigación, la AEPD solicita a la reclamada que le envíe en el plazo de un mes la siguiente información:

1. La decisión adoptada.
2. Acreditación de la respuesta al ejercicio de derechos.
3. Informe sobre las causas que han motivado la incidencia.
4. Informe sobre las medidas adoptadas para evitar situaciones similares.

No se recibió contestación alguna por parte del comercio online, por lo que fue sancionado con 1.000 euros por vulnerar el art.5 de la LOPDGDD del deber de confidencialidad, ya que, expuso a la vista de terceros datos personales de otros usuarios y con **una sanción de 2.000 euros por la infracción del el art. 32 del RGPD por no aplicar debidamente las medidas técnicas y organizativas adecuadas para garantizar la seguridad del tratamiento.**

IMPORTANTE

Se considera una infracción grave la quiebra de seguridad como consecuencia de la falta de la debida diligencia en la aplicación de las medidas adecuadas.

LA AEPD ACLARA

La videovigilancia en comunidades de propietarios regidas por la Ley de Propiedad Horizontal

La AEPD en su guía sectorial "Protección de datos y administración de fincas" recoge con carácter general conceptos y cuestiones básicas de la normativa de protección de datos. **Por otro lado, contempla también tratamientos específicos que frecuentemente llevan a cabo las comunidades de propietarios.**

Uno de estos supuestos específicos es el de la videovigilancia en la comunidades de propietarios. Cuando una comunidad pretenda llevar a cabo la instalación de videocámaras ha de tener en cuenta el siguiente requisito que se recoge en el art. 17.3 de la Ley de Propiedad Horizontal;

Se necesita un voto favorable de las tres quintas partes del total de propietarios que, a su vez, representen las tres quintas partes de las cuotas de participación.

Además, se recomienda que en el acuerdo alcanzado en la Junta se reflejen las características del sistema de videovigilancia, el número de cámaras y el espacio captado. En cuanto al espacio captado este no podrá captar imágenes de las zonas que no sean consideras comunes, ni imágenes de terrenos y viviendas colindantes.

El acceso a las imágenes solamente podrá realizarse por las personas que hayan sido designadas por la comunidad de propietarios y el sistema de grabación se ubicará en un lugar vigilado o de acceso restringido. En ningún caso será accesible a los vecinos mediante canal de televisión comunitaria.

IMPORTANTE

Las imágenes se conservarán durante el plazo máximo de un mes desde su captación, salvo que deban conservarse para la acreditación de delitos.

ACTUALIDAD LOPD

La AEPD publica una guía sobre requisitos en auditorías de tratamientos que incluyen Inteligencia Artificial

Fuente: AEPD

(Madrid, 12 de enero de 2021). La Agencia Española de Protección de Datos (AEPD) ha publicado la guía Requisitos para auditorías de tratamientos de datos personales que incluyan Inteligencia Artificial, un documento que ofrece orientaciones y un listado de posibles **objetivos de control y controles** específicos que podrían incorporarse en estas auditorías desde una perspectiva de protección de datos.

La realización de tratamientos de datos personales en los que se utiliza Inteligencia Artificial (IA) para realizar análisis e inferencias exige que se aplique un modelo de desarrollo maduro que proporcione garantías de calidad y privacidad. El **impacto que podrían tener los tratamientos** basados en IA en los derechos y libertades de los ciudadanos pone de manifiesto la **necesidad de establecer medidas de control efectivo**, corrección, responsabilidad, rendición de cuentas, gestión del riesgo y transparencia relativas a los sistemas y a los tratamientos de los datos en los que se utilice.

El Reglamento General de Protección de Datos (RGPD) establece en su artículo 24 la obligación por parte de aquellos que tratan datos de aplicar "medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento". Estas medidas han de ser seleccionadas "teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas" y una de esas herramientas para "garantizar y poder demostrar" el cumplimiento del RGPD es la realización de auditorías. Ello requiere disponer de **criterios objetivos** diseñados para ejecutar la auditoría de componentes de IA desde una perspectiva de protección de datos.

El documento recoge objetivos como inventariar el algoritmo auditado, identificar las responsabilidades y cumplir con el principio de transparencia; identificar las finalidades, analizar la proporcionalidad y necesidad del tratamiento y los límites en la conservación de los datos; asegurar la calidad de los datos y controlar posibles sesgos y verificar y validar las acciones realizadas y los resultados obtenidos dando cumplimiento al principio de responsabilidad activa del RGPD, entre otros.

El texto está dirigido, principalmente, a responsables y encargados que han de auditar tratamientos que incluyan componentes basados en IA, de cara a garantizar y poder demostrar el cumplimiento de obligaciones y principios en materia de protección de datos a los que están sujetos; a los desarrolladores que quieran ofrecer garantías sobre sus productos y soluciones; a los Delegados de Protección de Datos (…)

Puede ver más información en el siguiente enlace

Requisitos para Auditorías de Tratamientos que incluyan IA

Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial

EL PROFESIONAL RESPONDE

¿Cuáles son los principales amenazas en ciberseguridad a los que se enfrenta la empresa?

Durante este insólito 2020, los ataques más frecuentes han sido los siguientes:

1º Ransomware; A través del cual se pretende cifrar la información para pedir luego un rescate. El medio más frecuente ha sido el phishing, suplantando la identidad de diferentes instituciones como; OMS, Ministerio de trabajo, Servicio Público de Empleo(..)

La última versión es que primero exfiltran la información antes de cifrarla pidiendo un rescate a la empresa amenazando con publicarla sino lo realizan.

2º Robo de credenciales; El modo de proceder también ha sido el phishing, así obtienen las credenciales de los usuarios y acceden a sus cuentas bancarias y servicios en la nube. Por ejemplo, el robo de credenciales de Microsoft 365 les permite configurar palabras clave que se reenvían a una cuenta de correo con la finalidad de preparar un fraude al CEO.

3º Ataques a escritorios remotos; Debido a la situación actual de pandemia y la necesidad del teletrabajo, muchas empresas publicaron los escritorios remotos de los empleados en Internet, sin una seguridad adicional como puede ser una VPN.

4º Fraudes al CEO; la situación de teletrabajo ha hecho que exista un mayor aislamiento del personal, con lo cual han aumentado los casos de suplantación del Director General.

IMPORTANTE

Los ataques cada vez son más sofisticados, en EEUU se han utilizado softwares avanzados que son capaces de imitar el tono de voz del CEO.