Boletín 04/23

LOPD EN LA EMPRESA

EL RGPD UE 2016/679 EN APLICACIÓN

La seguridad de los datos personales (I)

Hoy en día, cada vez se producen más brechas de seguridad en el entorno digital que afectan a los datos personales de los cuáles son responsables las entidades. En el RGPD se dedica una sección completa a la seguridad de los datos personales.

El responsable del tratamiento y el encargado del tratamiento están obligados por la norma 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.

Para conocer el alcance de los riesgos es preciso que tanto el responsable del tratamiento como el encargado realicen un análisis de riesgos sobre los activos de la entidad. Ese análisis de riesgos nos proporcionará las medidas técnicas y organizativas más adecuadas para garantizar la mayor seguridad posible en el tratamiento de los datos personales.

Estas medidas, tal y como recoge el RGPD, podrían ser, la seudonimización y el cifrado de datos personales; un proceso de verificación, evaluación y valoración de las medidas (auditorías), la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

Contenido

IMPORTANTE

El responsable y el encargado de tratamiento deben realizar un exhaustivo análisis de riesgos para aplicar las medidas de seguridad adecuadas.

SANCIONES DE LA AEPD

Sancionado un autónomo con 1.500€ por enviar correos electrónicos comerciales sin copia oculta

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00343-2022.pdf, se sanciona a un autónomo por enviar correos comerciales sin copia oculta.

La parte reclamante denunció la recepción de un correo electrónico publicitario remitido por el reclamado a múltiples destinatarios sin utilizar la función de copia oculta. Se le solicitó, además, que se le diera de baja para recibir más correos electrónicos.

La Subdirección General de Inspección de Datos realizó las actuaciones previas de investigación para esclarecer los hechos. Se envió un requerimiento al reclamado el cuál alegó que se trataba de un error humano.

La AEPD desestimó dichas alegaciones, ya que las medidas de seguridad deben adoptarse en atención a todos y cada uno de los riesgos presentes en el tratamiento de datos de carácter personal, incluyendo entre estos riesgos, el factor humano. **El envío del correo electrónico sin copia oculta supone un quebrantamiento de las medidas técnicas y organizativas vulnerando la confidencialidad de los datos.**

Se ha vulnerado, por lo tanto, el art.5.1. f del principio del deber de confidencialidad y el art.32 de la seguridad del tratamiento, puesto que se ha producido un incidente de seguridad al remitir el correo electrónico a un número elevado de destinatarios, sin la función de copia oculta.

El responsable y el encargado del tratamiento han de aplicar las medidas técnicas y organizativas adecuadas, teniendo en cuenta la técnica, los costes de aplicación, y finalidad del tratamiento.

IMPORTANTE

Se considera una infracción muy grave el tratamiento de datos sin aplicar los principios generales del tratamiento, tales como el de licitud, lealtad y transparencia

LA AEPD ACLARA

Videovigilancia y protección de datos personales (I)

En este boletín y siguientes afrontaremos el uso de la videovigilancia en diferentes ámbitos y como afecta a la protección de datos personales. En el sitio web de la AEPD, en el espacio denominado "Áreas de actuación", podemos encontrar mucha información sobre la videovigilancia.

Con carácter general, estas serían las indicaciones básicas que han de conocerse en cuanto al tratamiento de imágenes:

1. No están sometidas a la normativa de protección de datos el tratamiento de imágenes en el ámbito exclusivamente personal o doméstico por una persona que capte el interior de su propio domicilio.
2. **No se podrán obtener imágenes de espacios públicos con fines de seguridad, esta actividad está reservada en exclusiva a las Fuerzas y Cuerpos de Seguridad.** En ningún caso se pueden captar imágenes en baños, vestuarios o lugares análogos.
3. Las imágenes serán conservadas durante un plazo máximo de un mes desde su captación, transcurrido el cual se procederá al borrado.
4. Si se produjese la grabación de un delito o infracción administrativa que debe ser puesta a disposición de una autoridad, las imágenes se acompañarán a la denuncia y no podrán ser utilizadas para ningún otro propósito.
5. **En todos los casos se deberá informar de la existencia del sistema de videovigilancia con un cartel suficientemente visible en los accesos a las zonas videovigiladas.**

IMPORTANTE

El responsable y/o encargado del tratamiento deberán adoptar las medidas de seguridad de carácter técnico y organizativo, según el análisis de riesgos realizado previamente.

ACTUALIDAD LOPD

La AEPD publica unas orientaciones para Administraciones Públicas ante el riesgo de brechas de datos personales

Fuente: AEPD

(Madrid, 28 de marzo de 2023) La Agencia Española de Protección de Datos (AEPD) ha publicado hoy Orientaciones para tratamientos que implican comunicación de datos entre Administraciones Públicas ante el riesgo de brechas de datos personales, un documento destinado al sector público que aborda la **necesidad de gestionar los riesgos** derivados del tratamiento de cantidades masivas de datos personales, y su intercambio entre AAPP, tanto para los derechos y libertades de las personas como para la propia sociedad en su conjunto.

Dirigido a organismos públicos y a sus delegados de protección de datos, el documento está centrado en aquellos tratamientos en los que, debido al elevado volumen de datos personales y por la interconexión permanente entre sistemas de las Administraciones, son susceptibles de sufrir brechas masivas de datos personales de alto riesgo para los derechos fundamentales.

Las Administraciones Públicas, al igual que todos los responsables del tratamiento, han de asumir que las brechas de datos personales podrían producirse y que las medidas de seguridad no garantizan una protección total. Por lo tanto, deben implementar desde el diseño del tratamiento medidas y acciones específicas para minimizar el posible impacto personal y social de una brecha en caso de producirse. En 2021, la Agencia recibió 163 notificaciones de brechas personales provenientes del sector público, y en 2022 esa cifra se incrementó un 49% hasta las 243.

Una gestión eficaz de los riesgos implica la actuación coordinada de las entidades implicadas en el tratamiento, un estudio conjunto de los distintos escenarios de brechas masivas en caso de fallo de las medidas de seguridad y la adopción de los procedimientos, técnicas de protección de datos y medidas de seguridad específicas y adecuadas para minimizar su impacto sobre los derechos fundamentales. Como material de ayuda, las Orientaciones incluyen un listado de medidas preventivas de detección, respuesta, revisión y supervisión que se podrían implementar en el marco de este tipo de tratamientos.

Puede ver más información en el siguiente enlace

Orientaciones para tratamientos que implican comunicación de datos entre Administraciones Públicas ante el riesgo de brechas de datos personales

EL PROFESIONAL RESPONDE

Proteger la información de la empresa: valoración del riesgo (II)

La clasificación de la información se puede establecer en varias categorías, confidencial; interna y pública, tal y como pudimos ver en el anterior boletín. Esta clasificación resulta fundamental para valorar la criticidad de la información y determinar así su riesgo específico para enfocar las medidas más adecuadas.

La realización de un análisis de riesgos resulta imprescindible para determinar las medidas técnicas y organizativas necesarias para proteger la privacidad. Este análisis consiste en averiguar el nivel de riesgo que la empresa está soportando. Para ello, tenemos que conocer los siguientes conceptos:

- **La información:** es el activo principal que debemos proteger, también tenemos que considerar otros activos en la empresa, como la infraestructura informática, equipos auxiliares, redes de comunicaciones, instalaciones y personas.
- **Las amenazas**: para valorar los daños en la información, procesos y soportes, podemos hacernos las siguientes preguntas; ¿qué valor tiene este activo para mi empresa? ¿cuánto cuesta su mantenimiento? ¿cuánto costaría recuperarlo o volverlo a generar?
- **Las vulnerabilidades**: aquellas frente a las que se debe proteger a los sistemas de información dependerán de la naturaleza del activo, por ejemplo, aplicaciones informáticas, que por su diseño son más inseguras que otras y el personal sin la formacion adecuada.

IMPORTANTE

Debemos proteger la información de riesgos que puedan afectar a una o varias de sus tres principales propiedades: confidencialidad; integridad y disponibilidad.