PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

www.prodasur.es
prodasur@prodasur.es
952 60 37 70

Boletín 11/24

EL RGPD UE 2016/679 EN APLICACIÓN

Deber de confidencialidad en la protección de datos

El deber de confidencialidad es esencial en la gestión de datos personales. Este principio, que se regula en el artículo 5.1.f del Reglamento General Europeo de Protección de Datos (RGPD), señala que los datos personales deben ser tratados de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilegal y contra su pérdida, destrucción o daño accidental.

Esto implica que las entidades y personas que traten información personal están obligadas a proteger su confidencialidad, previniendo accesos no autorizados y garantizando la confidencialidad de los datos personales.

Nuestra Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), en su artículo 5, refuerza esta obligación, subrayando que toda persona que intervenga en el tratamiento de datos personales debe respetar el deber de secreto, incluso después de finalizar su relación con el responsable o encargado del tratamiento.

La obligación general del deber de confidencialidad contenida en la normativa de protección de datos es complementaria con el deber de secreto profesional de conformidad con su normativa aplicable.

Contenido

IMPORTANTE

Los responsables, encargados del tratamiento y cualquier persona involucrada en el tratamiento de datos deben mantener la confidencialidad en todas las etapas del proceso.

SANCIONES DE LA AEPD

Sancionada una empresa con 10.000 € por no incluir la política de privacidad en su página web

En la resolución de la AEPD https://www.aepd.es/documento/ps-00546-2023.pdf se sanciona con 10.000€ a una empresa por no cumplir con el principio de transparencia y el deber de informar.

La reclamante manifiesta que la empresa ya había sido sancionada por la AEPD en una ocasión anterior. Aún habiendo transcurrido un largo tiempo desde su primera reclamación, la web cuestionada continuaba sin tener disponible ningún aviso legal y la información sobre la empresa seguía siendo incorrecta.

El formulario de la web de la empresa sancionada no proporcionaba información clara sobre el responsable del tratamiento cuando recogía datos personales. No existía un enlace directo a la "Política de Privacidad" o "Aviso Legal" que permitiera al usuario acceder a dicha información. El artículo 13 del RGPD exige que el responsable proporcione al interesado un fácil acceso a la información completa sobre el tratamiento de sus datos personales.

Se verificó que la entidad obligaba a los usuarios a aceptar una política de privacidad con información errónea.

La sanción ascendió a 10.000 € ya que existía un agravante debido a una sanción anterior (PS/00086/2023) por deficiencias similares en la "Política de Privacidad".

El término "de fácil acceso" en una web significa que la información debe ser fácilmente reconocible y accesible, por el usuario, a través de enlaces directos o respuestas claras.

IMPORTANTE

El principio de transparencia requiere que la información sea clara, concisa, comprensible y accesible, utilizando un lenguaje sencillo y visualizable.

LA AEPD ACLARA

Uso de videocámaras para seguridad y otras finalidades: Comunidades de propietarios (I)

En la página de la AEPD en el área de actuación de videovigilancia podemos acceder a información relevante sobre la utilización de las cámaras de grabación en diferentes entornos.

En este boletín abordaremos cuáles son los principales requisitos que ha de cumplir una comunidad de propietarios para instalar cámaras de videovigilancia en zonas comunes.

1º **Legitimación para la instalación**: Será necesario un acuerdo favorable de las 3/5 parte del total los propietarios. Se recomienda que en ese acuerdo se reflejen las características del sistema de videovigilancia.

2º **Derecho de información**: Se instalarán en los distintos accesos a la zona videovigilada, y en un lugar visible, uno o varios carteles. En el que se indique, la identidad del responsable y ante quién y donde dirigirse para ejercer los derechos de protección de datos.

3º **Instalación**: Las cámaras solamente podrán captar imágenes de las zonas comunes de la comunidad. La vía pública no podrá ser grabada, salvo que sea imprescindible, y en ese caso, solamente se podrá grabar una franja mínima de los accesos a los inmuebles. No se podrán captar imágenes de terrenos ni viviendas colindantes. **En las cámaras orientables o que tienen *zoom*, hay que instalar máscaras de privacidad para no grabar propiedades ajenas.**

IMPORTANTE

El sistema de grabación debe estar en un área restringida, accesible solo para personal autorizado. Las imágenes se conservarán hasta un mes antes de ser borradas.

ACTUALIDAD LOPD

La AEPD elabora unas orientaciones sobre obligaciones y responsabilidades por el uso de dispositivos móviles en los centros educativos

Fuente: AEPD

(17 de septiembre de 2024). La Agencia Española de Protección de Datos (AEPD) ha publicado unas orientaciones sobre 'Responsabilidades y obligaciones en la utilización de dispositivos digitales móviles en la enseñanza infantil, primaria y secundaria', en las que analiza las implicaciones que puede tener el uso de esta tecnología y qué principios deben cumplir los centros docentes y las autoridades educativas para que el tratamiento de datos personales derivado del uso de estos dispositivos respete la normativa de protección de datos. Estas orientaciones están dirigidas a las autoridades educativas, equipos directivos de centros escolares, docentes y familias.

Actualmente, en los centros educativos es frecuente el uso de teléfonos móviles o tabletas, a menudo propiedad del alumnado o sus familias. En muchos casos, los servicios y productos que se utilizan en los centros como método didáctico tratan grandes volúmenes de datos personales que se alojan en la nube por parte de terceros más allá del propio centro o autoridad educativa.

Las orientaciones recogen las situaciones que pueden darse con relación a la regulación del uso de teléfonos móviles en los centros (que se prohíba o limite la posibilidad de llevar dispositivos; que se usen en el aula a requerimiento del profesorado o que exista ausencia de regulación sobre su uso) y las responsabilidades que conllevan cada una de ellas.

Asimismo, la Agencia señala que la utilización de teléfonos inteligentes y otros dispositivos digitales con fines educativos, propiedad del alumnado y sus familias, puede generar tratamientos de datos que **afecten gravemente a sus derechos y libertades**, en concreto a su derecho a la no discriminación y a la educación; a la vida privada y familiar; a la integridad física y psíquica del menor, y a la protección de sus datos personales, además de a su desarrollo integral como personas. La Agencia recoge **ejemplos y buenas prácticas** para proteger a los menores ante los **riesgos relacionados con el acceso a contenidos para adultos**, como pueden ser el contacto con personas que puedan ponerlos en peligro, la contratación de productos y servicios, la monetización de sus datos personales, la inducción a comportamientos adictivos que afecten a su integridad física o mental.

Puede ver más información en el siguiente enlace:

RESPONSABILIDADES Y OBLIGACIONES EN LA UTILIZACIÓN DE DISPOSITIVOS DIGITALES MÓVILES EN LA ENSEÑANZA INFANTIL, PRIMARIA Y SECUNDARIA

EL PROFESIONAL RESPONDE

Prevención *ransomware*: pasos para reconocer un ataque de ingeniería social

La premisa más importante para evitar cualquier tipo de ciberamenaza es conocer como funcionan cada uno de los ataques a los que todos podemos estar expuestos. En este caso, vamos a analizar como funciona un ataque de ingeniería social.

Lo primero de todo, debemos saber que no difieren mucho de los timos presenciales, el ciber criminal emplea un proceso similar al del estafador en persona; primero realiza un reconocimiento, luego establece contacto, genera confianza, y finalmente manipula a su víctima para alcanzar su propósito y alejarse de la situación sin despertar sospechas.

Los atacantes usan técnicas manipulación aprovechándose de las siguientes situaciones:

- Respeto a la autoridad: el atacante se hace pasar por un organismo público o un miembro de las Fuerzas y Cuerpos de Seguridad del Estado.
- Disposición a colaborar o ayudar en los entornos laborales y comerciales.
- El miedo a perder oportunidades, como es el caso de solicitudes de pago para acceder a trabajos, premios o recompensas.
- Del ego de los individuos, mediante mensajes que notifican falsos premios o logros, instando a realizar acciones que de otro modo no se aceptarían.
- Creación de situaciones de urgencia que aprovechen la falta de experiencia, pereza o ingenuidad de las personas.

IMPORTANTE

Tras ganarse la confianza de la víctima, el atacante la manipula para obtener datos sensibles, como credenciales o información privada, para inducirla a realizar acciones como instalar software o enviar correos.