PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 10/24

EL RGPD UE 2016/679 EN APLICACIÓN

Tratamiento de categorías especiales de datos (II)

El artículo 9.2 del Reglamento General de Protección de Datos (RGPD) establece las excepciones a la prohibición general de tratar categorías especiales de datos personales. Estas excepciones permiten su tratamiento bajo ciertas condiciones:

Consentimiento explícito: El interesado debe otorgar su consentimiento, siempre y cuando la normativa de protección de datos no indique que, en algunos casos, el tratamiento es imposible, incluso cuando el interesado lo haya facilitado.

Obligaciones laborales y de seguridad social: El tratamiento es necesario para cumplir obligaciones en estos ámbitos.

Intereses vitales: Se permite el tratamiento si es necesario para proteger intereses vitales cuando la persona no esté capacitada para dar su consentimiento.

Actividades legítimas de fundaciones o asociaciones sin ánimo de lucro: Se permite tratar los datos personales cuando éstos no se comuniquen fuera de estas asociaciones.

Intereses públicos sustanciales: En casos de interés público, como investigaciones científicas o estadísticas, bajo medidas adicionales de protección.

Fines médicos, laborales o asistenciales: siguiendo la ley o contratos sanitarios.

Contenido

IMPORTANTE

El tratamiento de datos con fines médicos debe realizarse por un profesional sujeto a secreto profesional o bajo su responsabilidad, conforme a la normativa vigente.

SANCIONES DE LA AEPD

Sancionada una asesoría con 145.000 por no aplicar medidas de seguridad en un USB robado

En la resolución de la AEPD https://www.aepd.es/documento/ps-00084-2022.pdf se sanciona con 145.000€ a una asesoría por no implementar las medidas de seguridad adecuadas.

La entidad sancionada comunicó debidamente una brecha de seguridad ante la AEPD, por el robo de una mochila de un trabajador que contenía, entre otros objetos, un USB con datos personales sin cifrar. En el procedimiento de investigación, la AEPD solicitó un listado de las medidas de seguridad aplicadas a cada uno de los dispositivos robados. En este caso, el USB no estaba cifrado por lo que la AEPD consideró que se habían vulnerado los siguientes artículos del RGPD:

Artículo 5.1.f RGPD: Se vulnera el principio de confidencialidad por no tener aplicada el USB ninguna medida de cifrado o cualquier otra dirigida a imposibilitar el acceso a su contenido por parte de terceros no autorizados.

Artículo 32 RGPD: La entidad reclamada alegó que había realizado el análisis de riesgos y que, en base a ello, había aplicado las medidas de seguridad necesarias. Sin embargo, del proceso de investigación se dedujo que, respecto al USB sustraído, faltaban medidas de protección que evitaran el acceso por parte de terceros no autorizados.

El artículo 5.1.f del RGPD exige que los datos personales se protejan contra el acceso no autorizado, pérdida o daño, garantizando su integridad y confidencialidad.

IMPORTANTE

El incumplimiento de las medidas de seguridad puede ocurrir tanto por la falta de implementación de dichas medidas como por no aplicarlas con la diligencia adecuada.

LA AEPD ACLARA

Interés vital y protección de datos

En la página de la AEPD encontramos una publicación relativa al interés vital y protección de datos personales. El derecho a la protección de datos, según el Reglamento General de Protección de Datos (RGPD), no es absoluto. En algunas circunstancias, puede ceder ante otros derechos fundamentales, especialmente cuando se trata de proteger un interés vital para la vida del interesado o de terceros. Sin embargo, esta excepción debe aplicarse de forma limitada y bajo condiciones específicas.

1. El interés vital solo se justifica en situaciones donde la vida de una persona está en peligro y no existe otra base jurídica que permita el tratamiento de datos personales, como el consentimiento o el cumplimiento de obligaciones legales.
2. Se permite tratar datos de categorías especiales con el objetivo de salvaguardar la vida de una persona.
3. El tratamiento para proteger un interés vital ha de hacerse de forma proactiva, y gestionando el riesgo. Para ello han de estar previstos los mecanismos de registro de acceso y todo el procedimiento que conlleve el tratamiento de datos personales.

El RGPD estable por ello un sistema de ponderación que protege el interés esencial para la vida de una persona cuando existan conflictos de derechos.

IMPORTANTE

El tratamiento de datos personales aplicando el interés vital solo será posible en situaciones excepcionales como es el caso de emergencias o pandemias.

ACTUALIDAD LOPD

La AEPD publica un análisis sobre la protección de niños, niñas y adolescentes en el entorno digital

Fuente: AEPD

(2 de octubre de 2024). La Agencia Española de Protección de Datos (AEPD) ha publicado 'Internet seguro por defecto para la infancia y el papel de la verificación de edad' , en el que analiza cómo se puede proteger a niños, niñas y adolescentes en Internet sin que ello suponga una vigilancia e invasión de la privacidad de todos los usuarios, y sin exponer a la infancia a ser localizada y expuesta a nuevos riesgos. Este análisis se centra en la obligación de cumplimiento de los principios de protección de datos recogidos en el Reglamento General de Protección de Datos (RGPD), junto con otras regulaciones que complementan o profundizan en la protección de los menores.

El documento muestra **distintas estrategias de protección** a niños, niñas y adolescentes (NNA) en Internet, definiendo distintos casos de usos: protección ante contenidos inadecuados, entornos seguros para la infancia, consentimiento para el tratamiento de datos personales y diseño adecuado para la infancia. Cada caso de uso analizado está sujeto a marcos regulatorios diferentes y, como marco común, al RGPD en cuanto a tratamientos de datos personales.

El análisis publicado explica que, en la actualidad, buena parte de los servicios de Internet disponen de estrategias basadas, en el mejor de los casos, en reaccionar una vez detectado que ya se ha producido un daño o impacto. Una variación de ello es posibilitar a los proveedores de servicios de Internet el conocimiento de **quién es menor de edad**, como con la **creación de espacios o cuentas específicas para NNA**. Estas estrategias, añade, **precisan de una intervención intrusiva** en forma de vigilancia o perfilado que **vulnera la privacidad de todos los usuarios**: permiten tener al menor localizado y fácilmente accesible para cualquier actor malicioso, legitiman el tratamiento de datos personales adicionales de NNA, adaptan los mensajes para que tomen decisiones que no le corresponden o esconden propósitos de perfilado en relación con patrones engañosos o adictivos, fidelización, contratación, consumo o monetización de datos personales.

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.

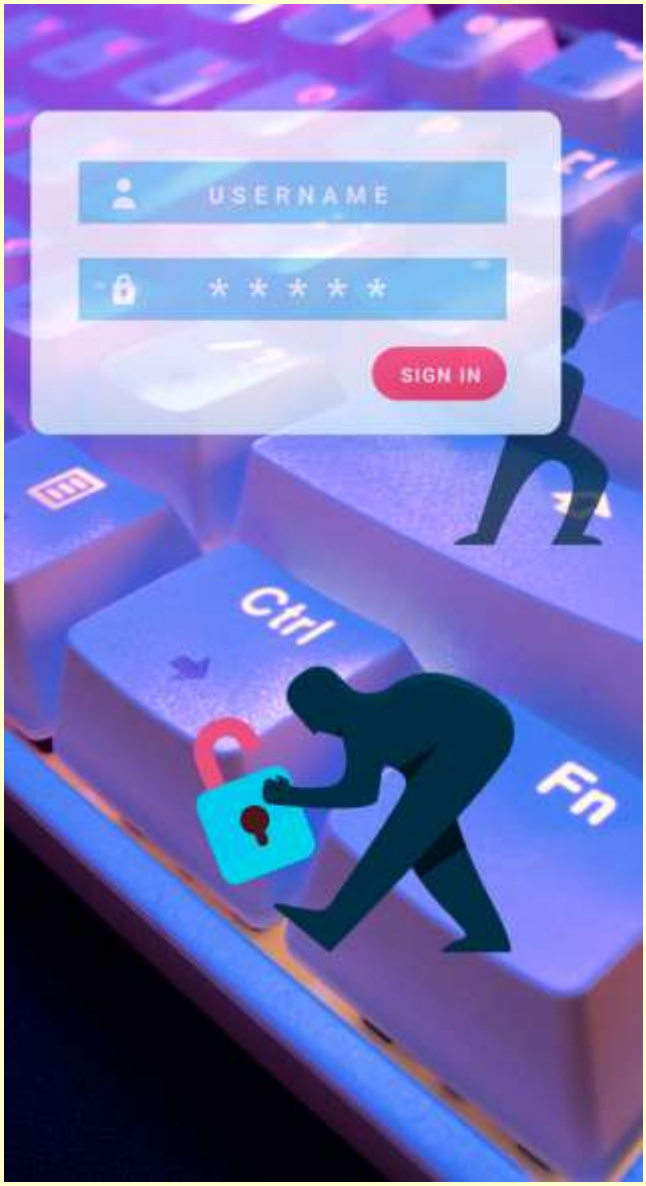
Puede ver más información en el siguiente enlace:

NOTA TÉCNICA: INTERNET SEGURO POR DEFECTO PARA LA INFANCIA Y EL PAPEL DE LA VERIFICACIÓN DE EDAD

EL PROFESIONAL RESPONDE

¿Cuáles son las principales vías para infectar a nuestros dispositivos? (II)

En este boletín, en el espacio de ciberseguridad, vamos a analizar cuáles son las principales vías para infectar a nuestros equipos. **Los ciberdelincuentes utilizan diversas estrategias para distribuir *malware*, como el *ransomware*, aprovechando vulnerabilidades en sistemas y engañando a los usuarios**:



Vulnerabilidades de *software*: Aprovechan fallos de seguridad en sistemas operativos, aplicaciones o servidores *web* desactualizados para introducir *malware*.

Credenciales de acceso: Obtienen credenciales de administrador mediante técnicas de phishing o explotando malas prácticas, como el uso de contraseñas por defecto o incrustadas en el código fuente.

Ingeniería social: Engañan a los usuarios para que instalen el *malware* a través de correos falsos, redes sociales o servicios de mensajería.

Spam y enlaces maliciosos: Envían correos electrónicos con enlaces o archivos infectados, logrando que algunos usuarios hagan clic y se infecten.

Drive-by download y watering hole: Redirigen a las víctimas a sitios web comprometidos para que el *malware* se descargue sin que lo noten, aprovechando las vulnerabilidades del navegador.

IMPORTANTE

El *ransomware* se propaga aprovechando tanto debilidades técnicas como errores humanos. Proteger los sistemas y educar a los usuarios es clave para mitigar estos riesgos.