PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 12/24

EL RGPD UE 2016/679 EN APLICACIÓN

Información y transparencia (I)

Contenido

En el artículo 13 del Reglamento General de Protección de Datos (RGPD) se establecen los requisitos que deben cumplir los responsables del tratamiento al recopilar datos personales directamente del interesado. **Su objetivo principal es garantizar la transparencia en el tratamiento de datos y proporcionar al interesado toda la información necesaria para comprender cómo se usarán sus datos y cuáles son sus derechos.**

Los responsables del tratamiento tienen la obligación de facilitar esta información de manera clara, concisa y accesible al momento de obtener los datos. Entre los datos obligatorios, se incluye la identidad del responsable, la finalidad del tratamiento, la base legal, los destinatarios, los derechos del interesado (acceso, rectificación, supresión, entre otros), y si los datos se transferirán fuera del Espacio Económico Europeo.

Además, se destaca la importancia de informar sobre la existencia de decisiones automatizadas, como la elaboración de perfiles, y sus implicaciones.

Este artículo garantiza que las personas estén informadas sobre el uso de sus datos personales, fomenta la transparencia en las actividades de los responsables del tratamiento y refuerza el respeto por los derechos fundamentales.

IMPORTANTE

La falta de información al interesado sobre el tratamiento de sus datos personales, conforme a lo dispuesto en el RGPD y LOPDGD, supone una infracción muy grave.

SANCIONES DE LA AEPD

Sancionada una agrupación de electores por incumplimiento de la normativa de protección de datos

En la resolución de la AEPD https://www.aepd.es/documento/ps-00441-2023.pdf se sanciona con 4.000€ a una agrupación de electores por incumplimiento de la normativa de protección de datos.

La Agencia Española de Protección de Datos inició actuaciones de investigación tras una reclamación contra una agrupación de electores por posibles infracciones del Reglamento General de Protección de Datos (RGPD).

Se requirió a la agrupación que facilitara información esencial en relación con el deber de informar, en particular:

- Los datos identificativos del titular del blog.
- La política de privacidad y la información proporcionada según el artículo 13 del RGPD,
- El procedimiento para que los interesados ejerzan sus derechos,
- Copias de documentos clave como el Registro de Actividades de Tratamiento, el análisis de riesgos y las medidas de seguridad implantadas.

La falta de respuesta a estos requerimientos llevó a la AEPD a sancionar a la agrupación con 4.000 euros por no colaborar con la autoridad de control, incumpliendo su obligación de facilitar información relevante.

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

La autoridad de control puede ordenar al responsable, encargado o su representante que proporcionen información necesaria para sus funciones de investigación.

LA AEPD ACLARA

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

En la página de la AEPD en el área de actuación de videovigilancia se indican las referencias para una correcta instalación y uso de los sistemas de videovigilancia en las comunidades de propietarios.

Es importante implementar medidas estrictas que limiten el acceso y uso de estas imágenes para garantizar el cumplimiento normativo y proteger los derechos de las personas.

En primer lugar, el acceso a las imágenes debe restringirse únicamente al personal autorizado designado por la comunidad de propietarios o responsables del sistema. En ningún caso, las imágenes podrán ser accesibles a los vecinos a través de canales, como, por ejemplo, una televisión comunitaria.

Cuando se utilice una conexión a internet para acceder a las imágenes, esta debe estar protegida mediante credenciales únicas de usuario y contraseña, conocidas únicamente por las personas autorizadas. Además, se recomienda cambiar las contraseñas predeterminadas tras la instalación del sistema para evitar brechas de seguridad.

Los sistemas de grabación deben situarse en lugares seguros, con acceso restringido, y el contenido grabado solo podrá conservarse durante un máximo de un mes. Cualquier uso adicional, como la entrega de imágenes a autoridades judiciales o policiales, deberá realizarse bajo requerimiento formal en el marco de una investigación.

IMPORTANTE

El responsable del tratamiento debe implementar estos controles esenciales para garantizar la seguridad y el respeto a la privacidad.

ACTUALIDAD LOPD

La Agencia aprueba un nuevo sistema de mediación para agilizar las reclamaciones de protección de datos en materia de comunicaciones

Fuente: AEPD

(20 de noviembre de 2024). La Agencia Española de Protección de Datos (AEPD), ha aprobado el 'Código de conducta para la regulación de controversias de protección de datos en el sector de las comunicaciones electrónicas', promovido por las operadoras de telefonía de los grupos Orange, Telefónica, Vodafone y MásMóvil.

El código de conducta regula un **procedimiento de mediación** con el objetivo de que las dos partes, ciudadanos y entidades adheridas al código, alcancen un acuerdo sin tener que recurrir, si así lo decide el usuario, a un procedimiento administrativo o judicial para resolver su reclamación.

Los códigos de conducta, cuya adhesión es voluntaria pero **vinculante** para las entidades adheridas, constituyen una muestra de autorregulación que, en este caso, supone establecer un procedimiento gratuito para los ciudadanos para ofrecer una respuesta más ágil a las reclamaciones que puedan surgir frente a las entidades adheridas.

Este código de conducta entrará en vigor el próximo **17 de diciembre** y, a través del procedimiento que regula, los ciudadanos podrán plantear reclamaciones relacionadas con, entre otros casos, tratamientos de datos realizados sin base de legitimación, ejercicios de derechos no atendidos, inserción indebida en sistemas de información crediticia o contratación fraudulenta.

El RGPD establece que todos los códigos de conducta deben designar un **organismo de supervisión** que actúe con plena independencia tanto del promotor del código como de las entidades adheridas, y que debe ser acreditado por la autoridad de control. En este caso, el organismo acreditado por la Agencia para la supervisión y control de este código es el Jurado de la Publicidad, de la Asociación para la Autorregulación de la Comunicación Comercial (AUTOCONTROL).

AUTOCONTROL estudiará las reclamaciones que se reciban contra las entidades adheridas al Código, iniciando el procedimiento de mediación. La **duración máxima de este procedimiento será de 30 días**.

Puede ver más información en el siguiente enlace:

CÓDIGO DE CONDUCTA PARA LA RESOLUCIÓN DE CONTROVERSIAS DE PROTECCIÓN DE DATOS EN EL SECTOR DE LAS COMUNICACIONES ELECTRÓNICAS

EL PROFESIONAL RESPONDE

Prevención contra el *ransomware*: recomendaciones para evitar ser víctima de un ciberataque.

El *ransomware* es una de las amenazas más dañinas en el panorama de la ciberseguridad actual, busca manipular a las víctimas mediante tácticas de urgencia o miedo.

Recomendaciones para prevenir ataques de *ransomware*:

- **No interactuar con correos sospechosos**: Si recibimos un mensaje de un remitente desconocido o no solicitado, hay que eliminarlo sin abrirlo.
- **Analizar los enlaces antes de hacer clic:** Aunque provengan de personas conocidas, se tiene que verificar su autenticidad. Entrar solo en los servicios que muestren la *URL* completa antes de visitarlos.
- **Precaución con los archivos adjuntos:** Aunque el remitente sea de confianza, no se deben abrir archivos sin confirmar su legitimidad.
- **Mantener los sistemas actualizados:** Instalar las actualizaciones del sistema operativo y de sus herramientas de seguridad desde fuentes oficiales. El *software antimalware* siempre debe estar activo.
- **Implementar contraseñas seguras:** Las cuentas de usuario deben usar contraseñas fuertes y no tener permisos excesivos.
- **Controlar las aplicaciones instaladas**: Limitar la instalación de software a las aplicaciones necesarias, asegurándose de que provengan de fuentes oficiales.

IMPORTANTE

Protegerse del *ransomware* implica prudencia y buenas prácticas de seguridad. Mantenerse alerta y aplicar estas medidas reduce el riesgo. La prevención es más eficaz que enfrentar las consecuencias de un ataque.