Boletín 11 /23

LOPD EN LA EMPRESA

EL RGPD UE 2016/679 EN APLICACIÓN

Principio de limitación del plazo de conservación (III)

Los datos personales han de ser mantenidos por el responsable del tratamiento de forma que permita la identificación de los interesados durante no más tiempo del necesario para la finalidad por la que fueron recogidos. En el RGPD se incluye la posibilidad de que los datos personales se puedan conservar durante periodos más largos de tiempo en estos casos:

- fines de archivo en interés público
- fines de investigación científica o histórica
- fines estadísticos

Por otro lado, para establecer la limitación del plazo de conservación de los datos, el responsable del tratamiento tendrá que aplicar la normativa adecuada. Así, por ejemplo, en el caso de los datos personales recogidos para el tratamiento de la prevención del blanqueo de capitales, su normativa establece un plazo de conservación mínimo de 10 años. En el caso del mantenimiento de los datos del historial clínico la conservación mínima que se regula en su normativa es de cinco años contados desde la fecha del alta de cada proceso asistencial**. La conservación de los datos en relación con la prescripción de responsabilidades en materia de protección de datos será de tres años**. Durante este tiempo de conservación, el responsable aplicará medidas técnicas y organizativas adecuadas.

Contenido

IMPORTANTE

Será obligatorio el bloqueo de los datos cuando se solicite su supresión y estos no se puedan eliminar por el cumplimento de obligaciones legales.

SANCIONES DE LA AEPD

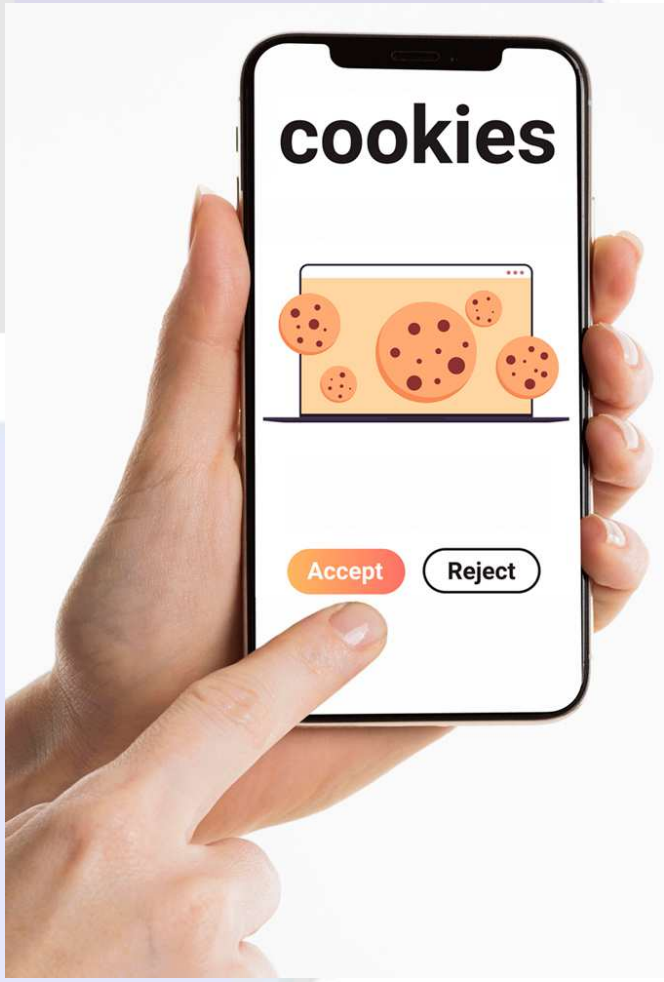
Sancionada una web con 12.000 € por el uso no adecuado de las cookies e informar indebidamente al usuario

En la resolución de la AEPD https:// https://www.aepd.es/documento/ps-00080-2023.pdf, se sanciona a una página web por no utilizar debidamente el uso de cookies e informar indebidamente en sus políticas de privacidad.

El interesado manifestó en su reclamación que en la política de privacidad del formulario de la web no se indicaba claramente a quién se destinaban los datos. Además, también incluyó en su reclamación que el responsable de la página estaba utilizando patrones oscuros de sobrecarga *(overloading)* y ocultación *(skipping)* en el diseño de la interfaz de usuario.

La AEPD señala el incumplimiento por parte del responsable del deber de informar, puesto que detalla de forma ambigua en su política de privacidad, los fines del tratamiento y la base jurídica. No se hace referencia tampoco, a la intención del responsable de transferir datos personales a un tercer país u organización internacional. **En cuanto al incumplimiento del uso de cookies la página web utiliza patrones oscuros de sobrecarga, en el configurador de cookies se hace referencia a un listado de proveedores y socios, desplegando una lista de 130 empresas, con la casilla premarcada de aceptar el tratamiento de datos por interés legítimo.** Además, no existe una política de cookies, la información se da de forma desordenada en la herramienta del gestor de cookies.

Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se está recogiendo, utilizando y consultando.



IMPORTANTE

La instalación de cookies que no sean necesarias para la intercomunicación de los terminales y la red en el equipo terminal siempre debe realizarse con el consentimiento previo del usuario.

LA AEPD ACLARA

Proteger a las personas en el mundo digital: Contenido mínimo de la comunicación (II)

En la infografía que publicaba la Agencia Española de Protección de datos en su página web sobre la comunicación a los afectados de una brecha digital, **se recoge el contenido mínimo de la comunicación**:

1. Naturaleza:

✓Se ha de describir que ha ocurrido si se trata de un ciberincidente, ciberataque, envío de datos por error, etc.

✓A qué datos ha afectado, si se trata de datos básicos, de contacto, email, usuario y contraseñas, copias de DNI, etc.

✓De qué manera se ha producido, si es por un acceso ilegítimo, datos extraídos, alterados, etc.

2. Consecuencias

✓Que impacto puede tener sobre las personas, si supone un menoscabo de los derechos fundamentales, fraude o daños físicos o psicológicos, entre otras.

✓A qué datos ha afectado, si se trata de datos básicos, de contacto, email, usuario y contraseñas, copias de DNI, etc.

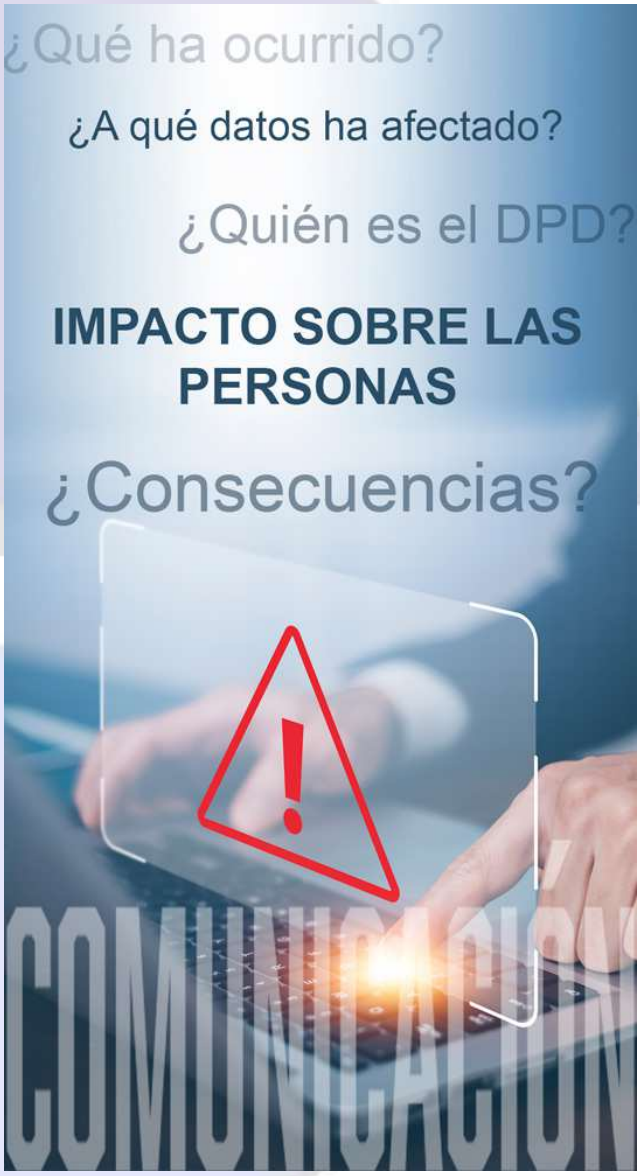
✓Si existen circunstancias agravantes, por ejemplo, porque la contraseña comprometida se usa en otros servicios, etc.

3. Medidas

✓ Identificar que medidas se han aplicado para minimizar las consecuencias sobre las personas.

4. Identificación

✓ Identificación comercial y pública del responsable y datos de contacto del DPD.



IMPORTANTE

En la comunicación no se deben omitir detalles relevantes, para que las personas puedan valorar el riesgo de forma adecuada.

ACTUALIDAD LOPD

Modificación del Código de conducta de AUTOCONTROL 'Tratamiento de datos en la actividad publicitaria'

Fuente: AEPD

(20 de octubre de 2023). La Agencia Española de Protección de Datos (AEPD), ha aprobado la modificación del Código de conducta 'Tratamiento de datos en la actividad publicitaria', promovido por la Asociación para la Autorregulación de la Comunicación Comercial (AUTOCONTROL). Esta modificación se debe esencialmente a la necesidad de adaptar su contenido a lo dispuesto en la Circular 1/2023 de la AEPD sobre la aplicación del artículo 66.1.b) de la Ley 11/2022 General de Telecomunicaciones, y se ha incorporado un sello que identifique a los adheridos al código.

En el código de conducta se regula **un procedimiento de mediación, de resolución extrajudicial de las controversias** que surjan entre los ciudadanos y las entidades adheridas al código con motivo de tratamientos de datos realizados en el ámbito de la actividad publicitaria.

La publicidad no deseada es una de las reclamaciones más frecuentes planteadas ante la Agencia, por lo que la presentación de estas a través de AUTOCONTROL y de este código de conducta, abierto a todas las empresas que desarrollen actividades publicitarias, permite establecer un procedimiento de mediación voluntario y gratuito para los ciudadanos para dar una respuesta más ágil a las reclamaciones que planteen frente a las entidades adheridas.

Este código de conducta **se aplica a los tratamientos de datos con fines publicitarios o que versen sobre publicidad** que realizan las entidades adheridas, como envío de comunicaciones comerciales, **incluidos aquellos en los que el interesado se encuentra en una lista de exclusión publicitaria**, promociones realizadas con objeto de recoger datos personales para utilizarlos con fines publicitarios, uso de cookies y tecnologías equivalentes para la realización de publicidad comportamental o elaboración de perfiles con fines publicitarios, entre otros.

Puede ver más información en el siguiente enlace:

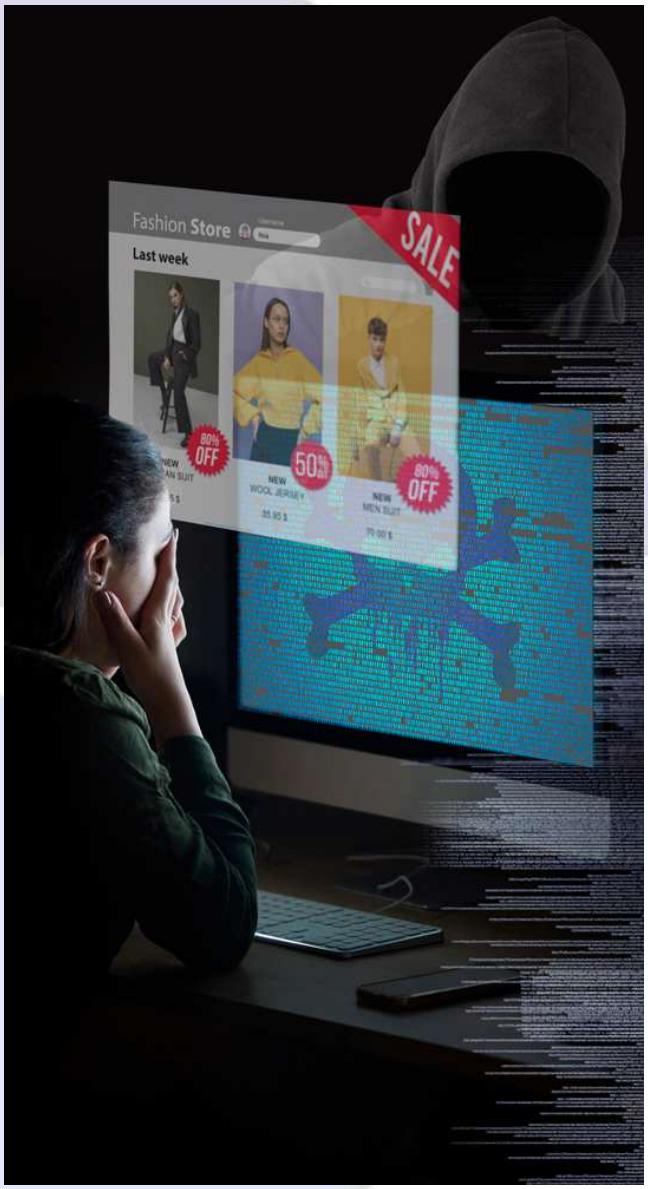
Funcionamiento del procedimiento

Listado de empresas adheridas

EL PROFESIONAL RESPONDE

¿Cómo pueden afectar los riesgos cibernéticos a nuestros clientes?

Durante los meses de noviembre y diciembre se producen muchas compras a través del comercio electrónico. Los ciberdelincuentes lo aprovechan para hacerse con datos personales.



Es importante conocer cuáles son los principales riesgos a los que debemos enfrentarnos si ofrecemos nuestros productos y servicios mediante este medio.

- El *defacement*; es un ataque que actúa sobre la apariencia de la página web para introducir modificaciones con diferentes objetivos, desde perjudicar la imagen de la empresa hasta alojar un *phishing* o introducir un *malware*.

- **Ataque de denegación de servicio**; puede llegar a bloquear la web, paralizando su actividad comercial.

- **Infección por *malware*;** si utilizamos en la página web *software* desactualizado o con vulnerabilidades no parcheadas.

Algunas de las medidas claves que se deben implementar para garantizar la seguridad de nuestro comercial *online* son las siguientes:

- Actualización de los sistemas para corregir vulnerabilidades que implementen nuevas medidas de seguridad.

- Aplicar sistemas de doble autenticación y usar contraseñas robustas.

- Realizar auditorías periódicas de seguridad para detectar áreas de mejora.

IMPORTANTE

La técnica de *egosurfing* para conocer qué información hay sobre nosotros o nuestra empresa en Internet puede ayudarnos a detectar campañas de suplantación.

AUTOR: JULIO CÉSAR MIGUEL PÉREZ