PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 05/23

EL RGPD UE 2016/679 EN APLICACIÓN

La seguridad de los datos personales (II)

Contenido

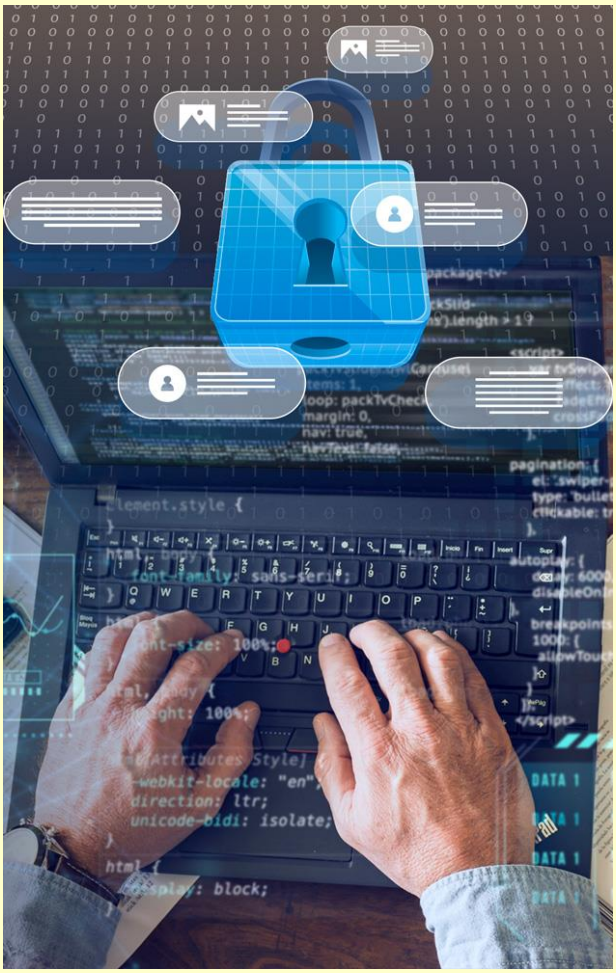
La seguridad de los datos personales implica una proactividad por parte de los responsables y encargados del tratamiento de los datos personales. Se han de aplicar las medidas de seguridad tanto técnicas y organizativas adecuadas para que, incluso, en el probable caso de que se produzca una brecha de seguridad, se pueda garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

¿Qué tipo de brechas de seguridad de datos personales se tienen que hacer frente? Es muy importante conocer la tipología y a qué dimensiones de la seguridad de los datos personales ha afectado la brecha.

A) Brecha de confidencialidad: aquellos casos en que no se tiene autorización para acceder a la información, revelación no autorizada o accidental de los datos personales.

B) Brecha de integridad: cuando se modifica la información original y se sustituye por otra causando un perjuicio al afectado.

C) Brecha de disponibilidad: se produce una pérdida de acceso accidental o no autorizada a los datos personales o bien se produce su destrucción.



IMPORTANTE

El responsable del tratamiento debe comunicar a la AEPD en el plazo máximo de 72hrs las brechas de seguridad que supongan un riesgo para los derechos y libertades de las personas.

SANCIONES DE LA AEPD

Sancionada una página web con 10.000€ por no tener la Política de privacidad y Política de cookies adecuada

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00393-2022.pdf, se sanciona a una página web por utilizar cookies analíticas sin consentimiento previo y no informar debidamente en su Política de Privacidad.

La reclamante interpuso una reclamación ante la AEPD indicando que en su página web no tenía Aviso Legal, además, la Política de Privacidad de la página no era correcta y no existía Política de cookies.

La AEPD admitió a trámite la reclamación y constató la siguiente información de la página web sancionada:

1º) En la Política de Privacidad de la página web no se está informando debidamente, puesto que no identifica correctamente al responsable del tratamiento de los datos personales. Para obtener más información, la página web te indica un correo electrónico de contacto. En este caso la sanción por incumplimiento del art.13 "Deber de informar" ascendió a 5.000€

2º) En la página web se instalan cookies no necesarias al entrar por primera vez en la web sin aceptar cookies y sin realizar ninguna acción. El banner informativo no permite rechazar las cookies y tampoco se permite realizar la gestión de cookies de forma granular o por grupos a través de un panel de control. Tampoco existía información en el banner de cookies referente a las finalidades de las cookies. La sanción ascendió a 5.000€

El responsable del tratamiento tiene que cumplir con el deber de informar al interesado, incluyendo entre esa información identidad, datos de contacto del responsable y en su caso del representante.

IMPORTANTE

Se considera una infracción muy grave la omisión del deber de informar al interesado acerca del tratamiento de sus datos personales.

LA AEPD ACLARA

Videovigilancia y protección de datos personales (I): Grabación en plazas de garaje

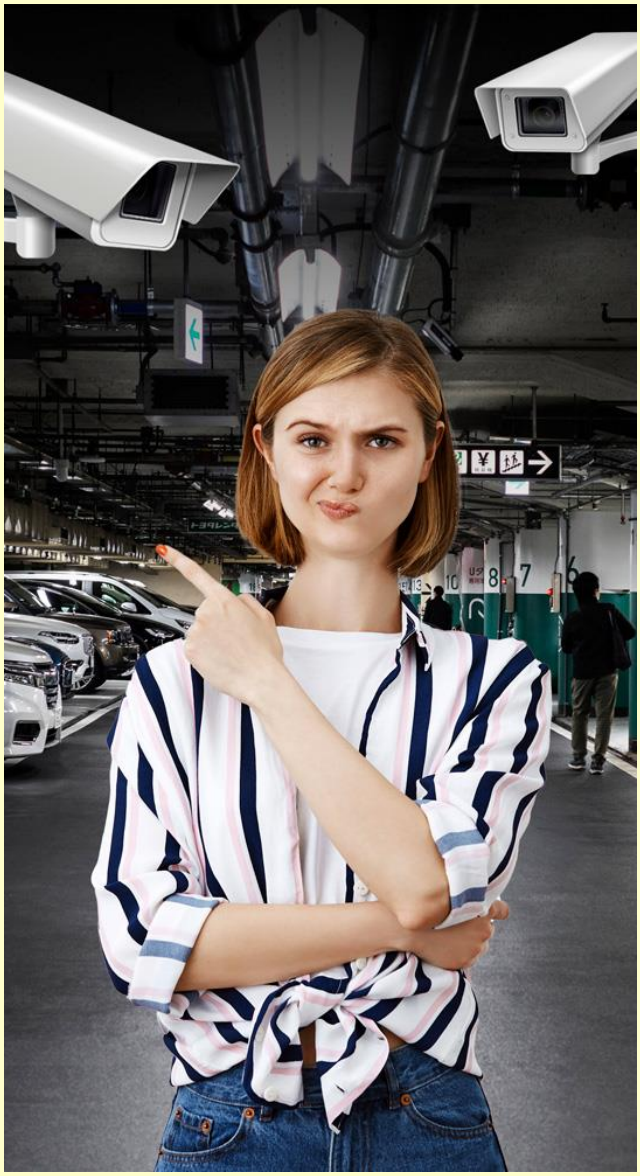
En este boletín y siguientes afrontaremos el uso de la videovigilancia en diferentes ámbitos y como afecta a la protección de datos personales. La AEPD ha emitido varios informes en relación con la videovigilancia instalada en las plazas de garaje.

En este informe emitido por el Gabinete Jurídico se resuelve una cuestión planteada por una comunidad de propietarios en la que se plantea si el propietario de una plaza de garaje puede instalar una cámara para evitar actos vandálicos.

La imagen de una persona es un dato personal, al igual que lo es cualquier información que permita determinar, directa o indirectamente, su identidad, por lo que la matrícula del vehículo también se puede considerar que es un dato personal.

La captación de imágenes en los espacios comunes de la comunidad de propietarios se podría legitimar en la esfera del interés público para garantizar la seguridad de las personas, bienes e instalaciones. Para ello, será necesario que se acuerde por mayoría según lo indicado en la Ley de Propiedad Horizontal.

Por otro lado, en este caso, el usuario del garaje solo podría instalar una cámara en su plaza, cuando se dirija exclusivamente a la zona donde tiene atribuido un uso exclusivo, sin grabar parte de la zona común de acceso a dichas plazas dentro del garaje y cumpliendo con la normativa de protección de datos.



IMPORTANTE

Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo que deban ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

ACTUALIDAD LOPD

Modificación de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

Fuente: AEPD

(9 de mayo de 2023). El Boletín Oficial del Estado (BOE) ha publicado hoy una modificación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Después de varios años desde la aplicación del Reglamento General de Protección de Datos (RGPD) y la entrada en vigor de la Ley Orgánica, la experiencia ha demostrado la necesidad de introducir modificaciones tanto en la tramitación de algunos procedimientos de la Agencia Española de Protección de Datos (AEPD) como en su Estatuto.

Ello se debe, en primer lugar, a la corrección de errores del RGPD publicada el pasado marzo en el Diario Oficial de la Unión Europea, de la que se desprende que no se debe considerar el apercibimiento como una sanción, tal y como se consideraba en el ordenamiento jurídico español. Dicha corrección requiere, dada la aplicación directa del RGPD, modificar la LOPDGDD para configurar el apercibimiento como una medida adecuada, de naturaleza no sancionadora, incluida dentro de los poderes correctivos de las autoridades de control.

En segundo lugar, el incremento y la mayor complejidad de los asuntos abordados por la Agencia en los procedimientos sancionadores muestra la necesidad de ampliar algunos de los plazos para resolver. Esta complejidad se ha visto acentuada además por la instauración por parte del RGPD del mecanismo de "ventanilla única", que requiere de un sistema de cooperación y coherencia entre las distintas autoridades de protección de datos de la UE en determinados casos. Por ello, la modificación contempla el aumento de nueve a doce meses en la duración máxima del procedimiento sancionador, y de doce a dieciocho meses en las actuaciones previas de investigación. Además, contempla otras modificaciones relevantes tales como, la forma de realizar actuaciones de investigación a través de sistemas digitales, para regular la opción de realizar no solo investigaciones presenciales sino también remotas. La posibilidad de establecer modelos de reclamaciones ante la Agencia, que serán publicados en el BOE y en la Sede electrónica de la AEPD serán de obligado cumplimiento al mes de su publicación y facilitarán la presentación de reclamaciones.

Puede ver la modificación completa en el siguiente enlace:

Información BOE

EL PROFESIONAL RESPONDE

¿Cómo puedo hacer para que mi empresa esté Ciberprotegida?

La empresa, lo primero que debería demostrar es un compromiso de seguridad. Para ello tiene que documentar y difundir lo que llamamos "la Política de seguridad". Cada empresa tiene sus propias características particulares en cuanto al número de empleados, dependencia con las tecnologías, área de actividad, etc. **Es importante, definir nuestra Política de seguridad mediante un Plan director de Ciberseguridad.**

Este Plan nos ayudará a determinar los aspectos siguientes en la empresa:

- Determinar el punto de partida de la empresa definiendo cuáles son los procesos críticos de la organización, los empleados y los equipos y activos esenciales para el funcionamiento de nuestra empresa.
- Determinar el nivel de seguridad que queremos alcanzar según las características de la empresa, el sector del negocio y los objetivos estratégicos, entre otros.
- **En su realización no tenemos que olvidarnos de la importancia del análisis de riesgos que permitirá la elaboración de planes personalizados y adecuados a cada empresa de forma particular.**

Este Plan de Ciberseguridad es una guía para conocer cuáles serán los productos de seguridad más adecuados para nuestra empresa, además de las normas de uso interno necesarias para aplicar los cambios en nuestra empresa y estar ciberprotegidos.

IMPORTANTE

La ciberseguridad supone un proceso que toda empresa debería implantar y revisar de forma periódica ya que las ciberamenazas evolucionan muy rápidamente.