PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 12/22

EL RGPD UE 2016/679 EN APLICACIÓN

Roles en la protección de datos: el delegado de protección de datos

Contenido

La última de las figuras que vamos a tratar en este boletín, pero no por ello la menos importante, es el rol del delegado de protección de datos, en adelante (DPD).

En el Reglamento Europeo de protección de datos está regulada su designación, posición y funciones. En nuestra Ley Orgánica la LOPDGDD existe un Capítulo completo dedicado a regular la figura del DPD.

Podemos destacar la función que el DPD tiene como interlocutor del responsable o encargado de tratamiento ante la AEPD y las autoridades autonómicas de protección de datos. En este sentido el DPD podrá inspeccionar los procedimientos que aplique la entidad relacionados con la protección de datos y emitir recomendaciones.

Además, algo novedosos que supuso la entrada en vigor de la LOPDGDD, es que cuando la AEPD o la autoridad competente reciba una reclamación de un afectado, podrá hacerla llegar al DPD para que la resuelva en el plazo de un mes. De igual modo, cuando el responsable y encargado de tratamiento hubieran designado un DPD, el interesado podrá dirigir su reclamación ante el DPD y éste deberá resolver en el plazo máximo de dos meses.

IMPORTANTE

Se considera una infracción grave la falta de designación del DPD cuando su nombramiento sea exigible por la normativa de protección de datos.

SANCIONES DE LA AEPD

Entidad inmobiliaria sancionada por no aplicar medidas de seguridad para proteger los datos personales

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00404-2022.pdf, se sanciona a una entidad inmobiliaria con 3.500 €.

La reclamación fue interpuesta por una persona que estaba interesada en uno de los anuncios publicados por la inmobiliaria. En el escrito de reclamación alegaba que el correo electrónico que recibió con la respuesta de la entidad estaba visible las direcciones de correo electrónico de otras personas. Como prueba relevante se acompaña a la reclamación la copia del correo electrónico recibido.

La directora de la Agencia Española de Protección de Datos admitió a trámite la reclamación presentada. Se procedió a solicitar información a la parte reclamada, pero ésta no contestó al requerimiento.

La entidad fue sancionada con 2.000 € por incumplimiento de uno de los principios regulados en el RGPD, el principio de integridad y confidencialidad. Al enviar un correo electrónico sin utilizar la copia oculta se está vulnerando la confidencialidad de los datos del resto de destinatarios. **Por otro lado, además, se le sanciona con 1.500 € por no cumplir con la obligación de aplicar las medidas técnicas organizativas apropiadas que garantizasen un nivel de seguridad adecuado** con el tratamiento de los datos personales, tal y como dispone el art. 32 del RGPD.

Las actuaciones negligentes de los responsables y encargados de tratamiento pueden incumplir importantes preceptos del RGPD como ocurre en esta resolución.

IMPORTANTE

El responsable y el encargado del tratamiento deben determinar las medidas técnicas y organizativas adecuadas al tratamiento.

LA AEPD ACLARA

¿Cuáles son los principales consejos a seguir antes de realizar una compra en Internet?

En las fechas en las que nos encontramos se hace necesario tener herramientas y consejos claves para que las compras por Internet sean lo más seguras posibles. La AEPD junto con otros organismos, han elaborado una guía de Compra segura en Internet, en la que se recogen aspectos esenciales a tener en cuenta.

Así, por ejemplo, en la guía encontramos un apartado con las recomendaciones que debemos seguir antes de realizar una compra o contratar:

1º **Recomendaciones de seguridad básicas:** Confirmar que el sistema operativo del dispositivo, todos los programas y aplicaciones instaladas estén actualizadas con la última versión.

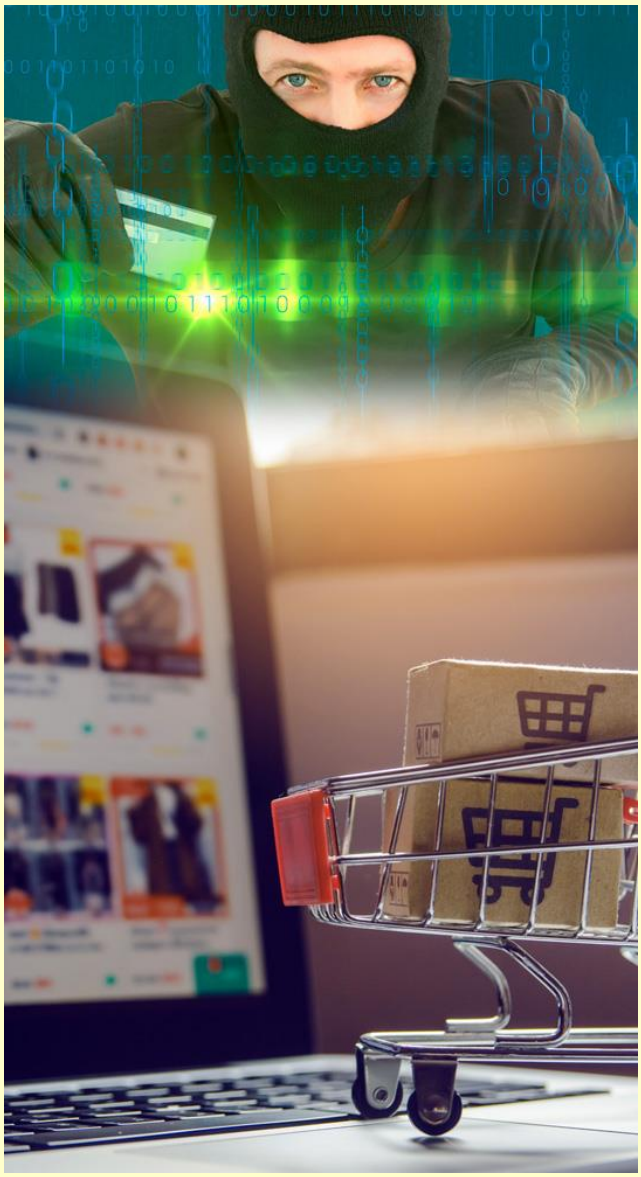
2º **Configuración de la red:** No conectar el dispositivo a una red *WiFi* pública para realizar transacciones de pago. Configurar adecuadamente el *WiFi* doméstico.

3º **Comprobar la información legal del comercio electrónico:** Aviso legal, Términos de uso, Política de privacidad y Condiciones generales de contratación.

4º **Verificar el titular y los datos del registro del dominio.** Comprobar si coincide con el que se identifica como responsable del sitio web.

5º **Comprobar que se tratan de comunicaciones seguras** (HTTPS).

6º **Sellos de confianza:** Los sellos de confianza dan fiabilidad y seguridad en los comercios electrónicos.



IMPORTANTE

Se recomienda sospechar de tiendas con precios por debajo del precio del mercado, sin información legal y el diseño web no transmita homogeneidad.

ACTUALIDAD LOPD

Neurodatos y neurotecnología: privacidad y protección de datos personales

Fuente: AEPD

Los recientes avances en neurotecnología e inteligencia artificial están permitiendo la aparición de un número creciente de dispositivos conectados que monitorizan la actividad cerebral para distintos propósitos. Estos dispositivos, ya disponibles en el mercado, y que se usan como accesorios portátiles con fines de entretenimiento o control de otros dispositivos, forman parte del conocido Internet de los Cuerpos (IoB, *Internet of Bodies*). Los datos cerebrales o neurodatos podrían identificar a los individuos, inferir estados emocionales, pensamientos o sentimientos, y revelar otras categorías especiales de datos.

Las interfaces cerebro-computador o BCI (*Brain Computer Interface*), son dispositivos que posibilitan la interacción directa entre el cerebro y un ordenador. Los BCI permiten interactuar con el mundo físico y virtual utilizando la mente. Para conseguirlo, recogen y miden las señales y la actividad del cerebro y con el software adecuado de captura y procesamiento, son capaces de extraer características de interés relacionadas con las intenciones y estado mental del usuario, y ejecutar acciones en consecuencia.

Aunque pueda parecer futurista, estamos hablando de tecnologías que ya están en el mercado de consumo. Grandes compañías (Snap, Valve, Meta, Apple, Samsung) están incorporando en sus productos tecnologías y dispositivos para captura de neurodatos.

Las primeras aplicaciones BCI tenían como objetivo proporcionar un canal de comunicación alternativo para usuarios con problemas de movilidad o del habla. Sin embargo, una serie de aplicaciones neuro-tecnológicas se ha abierto camino en el mercado y se ha integrado con un conjunto de dispositivos de consumo para usuarios sanos con diversos fines no clínicos. Estas aplicaciones buscan experiencias más inmersivas y completas en distintos usos (hogar inteligente, educación, neuromarketing, juegos y entretenimiento, internet, metaverso, seguridad y autenticación, ingeniería militar, etc).

Emotiv, Neurosky, Nextmind, OpenBCI, NexTem, Unicorn-bi, Brainattach, etc, ofrecen, a precios ya muy asequibles, un surtido de cascos inalámbricos para usarse en juegos y otras formas de entretenimiento, aplicaciones de marketing, monitorización o comunicación. Se comercializan también entornos de desarrollo software (incluso existen opciones de software libre) que facilitan la adquisición de datos recogidos por el BCI para desarrollar aplicaciones.

Puede ver más información en el siguiente enlace

Internet de los Cuerpos

Sección Innovación y Tecnología

EL PROFESIONAL RESPONDE

¿Cuáles son los ciberataques que puedo sufrir si tengo un comercio online?

Los comercios electrónicos están expuestos a una serie de ciberataques que ponen en peligro su reputación y actividad comercial. Es importante conocer cuáles son los principales para poder prevenirlos.

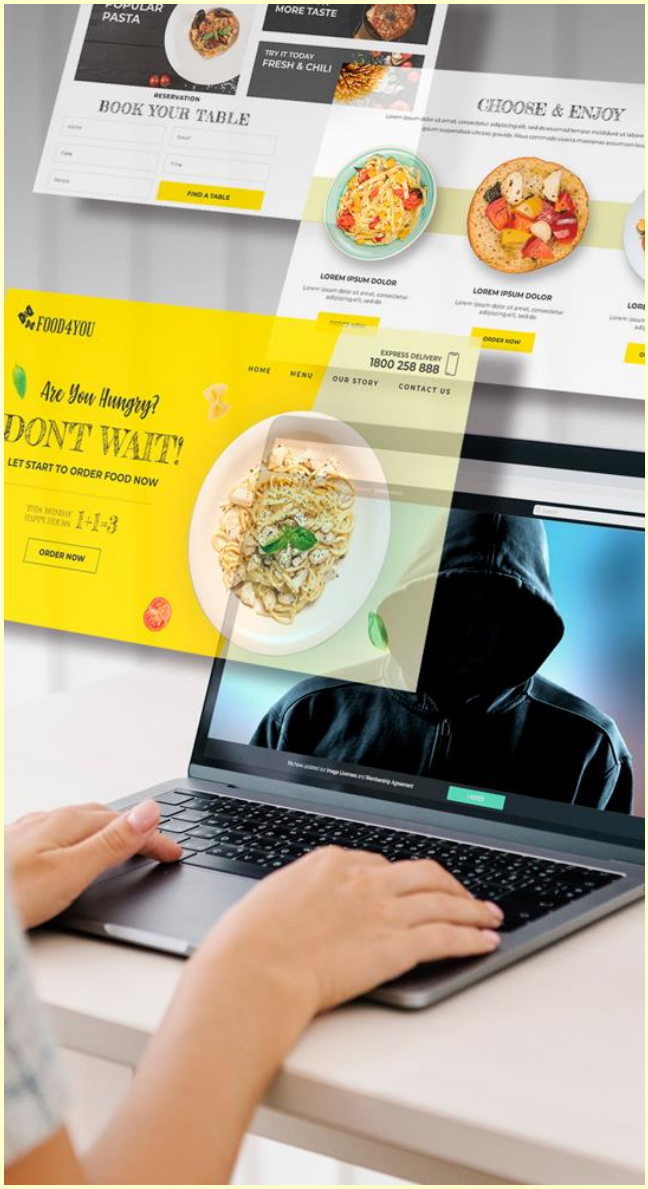
1º **El *defacement***: este ataque actúa sobre la apariencia visual de una página. Se reemplaza el sitio web alojado por uno propio, con el fin de cargar *malware* o eliminar archivos esenciales del servidor o dañar la imagen del comercio online. La mejor prevención en estos casos es incorporar una política de actualizaciones, una política de contraseñas seguras y realizar copias de seguridad periódicas.

2º **Ataque de denegación de servicio**: se puede bloquear la web y paralizar toda la actividad comercial. Para prevenir este tipo de ataques la entidad deberá aplicar elementos de protección perimetral.

3º **Bloqueo de acceso al panel de control** de la página web o servidor donde está alojado el comercio online.

4º **Infección por *malware*** cuando se utiliza en la página web software desactualizado o con vulneraciones no parcheadas.

Las recomendaciones para prevenir estos tipos de ataques entre otras, sería mantener actualizados los sistemas, realizar auditorías periódicas de seguridad y practicar la técnica de *egosurfing* que nos permite detectar campañas de suplantación a las entidades.



IMPORTANTE

La concienciación del personal laboral en materia de seguridad es una medida muy potente de seguridad.