PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 10/22

EL RGPD UE 2016/679 EN APLICACIÓN

Roles en la protección de datos: el encargado de tratamiento

Contenido

El encargado de tratamiento es otro de los roles imprescindibles a tener en cuenta en materia de protección de datos. Su definición la encontramos en el artículo 4.8 del RGPD: "***persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".***

En la normativa de protección de datos existen varios artículos que regulan y determinan las funciones del encargado del tratamiento. **En concreto, nuestra LOPDGDD, en el artículo 33, indica que, cuando el encargado utilice para su propia finalidad los datos facilitados por el responsable por cuenta de quién actúa, tendrá la consideración de responsable**. Esto significa que se le podrán aplicar las mismas cuantiosas sanciones que al responsable del tratamiento.

El contrato de acceso a datos, es el nombre que le damos al contrato celebrado entre el responsable del tratamiento y el encargado. **Su contenido íntegro se encuentra regulado en el artículo 28.3 del RGPD.** En él se deben indicar, entre otros aspectos, la duración, la naturaleza, la finalidad del tratamiento, el tipo de datos personales y categorías de interesados y las obligaciones y derechos del responsable. La falta de este contrato supone una falta grave.

IMPORTANTE

El encargado del tratamiento seguirá las instrucciones del responsable incluidas aquellas referidas a las transferencias internacionales.

SANCIONES DE LA AEPD

La Subdirección General de Inspección de Datos sanciona con 80.000€ a una empresa corredora de seguros

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00401-2022.pdf, la Subdirección General de Inspección de datos (SGID), inspeccionó de oficio a la entidad sancionada puesto que tenía conocimiento de actuaciones que podrían vulnerar la legislación en materia de protección de datos.

Varias entidades, responsables y encargados del tratamiento del sector seguros notificaron, a la División de Innovación Tecnológica de la AEPD, la publicación no autorizada de datos de sus clientes. La entidad sancionada, hizo público en distintos foros la venta de usuarios de una compañía de seguros dedicada al sector del automóvil, además de los registros con información personal de clientes españoles de una compañía de seguros.

La AEPD, consideró que la corredora de seguros, como proveedora de servicios de gestión e infraestructuras tecnológicas, no contaba con las medidas organizativas técnicas y tecnológicas apropiadas para impedir la exposición de los datos personales de los asegurados.

Las infracciones cometidas se refieren a los artículos 5.1.f del RPGD "principio de integridad y confidencialidad" y al artículo 32 del RGPD "seguridad del tratamiento". La cantidad ascendió a 80.000€. Finalmente, la sanción se redujo a 48.000€ aplicando las reducciones.

La recepción de una reclamación de brecha de seguridad no implica una sanción directa, se debe analizar la diligencia de responsables y encargados de las medidas de seguridad aplicadas.

IMPORTANTE

El responsable y encargado de tratamiento deben realizar un análisis de riesgos para determinar las medidas técnicas y organizativas apropiadas.

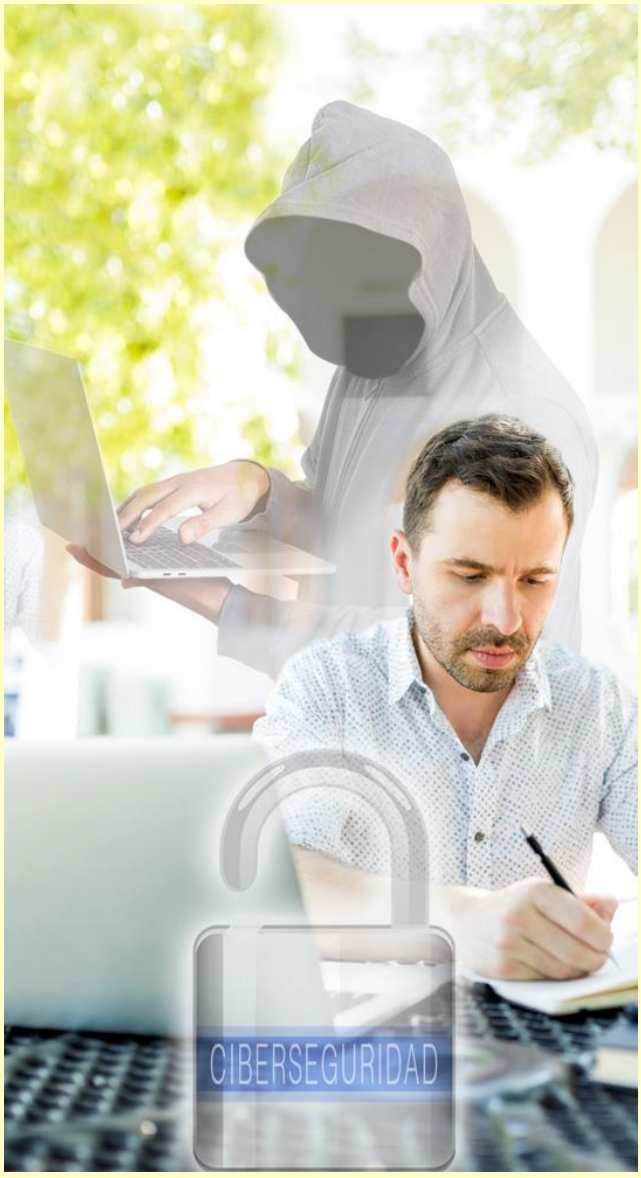
LA AEPD ACLARA

Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo (II)

Las recomendaciones editadas por la Unidad de Evaluación y Estudios Tecnológicos de la AEPD, se dirigen también, además de al responsable del tratamiento, al personal que participa en las operaciones de tratamiento.

Estas recomendaciones deben estar recogidas en la política de teletrabajo.

1. Se debe respetar la política de protección de la información en situaciones de movilidad definida por el responsable.
2. **Proteger el dispositivo. Se tienen que definir y utilizar contraseñas de acceso robustas**. No se deben descargar ni instalar aplicaciones que no hayan sido autorizados. Si el equipo utilizado para establecer la conexión remota es personal, debe evitarse simultanear la actividad personal con la profesional y definir perfiles independientes para cada tipo de tarea.
3. Garantizar la protección de la información. Evitar exponer la pantalla a la mirada de terceros. **Si se trabaja habitualmente desde lugares públicos, es recomendable utilizar un filtro de privacidad para la pantalla.** Si se trabaja con papel, minimizar la entrada y salida de documentación en este soporte.
4. **Guardar la información en los espacios de red habilitados.** No se debe bloquear o deshabilitar la política de copia de seguridad.
5. **Comunicar de forma inmediata cualquier anomalía que afecte a la seguridad de la información.**



IMPORTANTE

Una vez concluida la jornada laboral en situación de movilidad debe desconectarse la sesión de acceso remoto y apagar o bloquear el acceso al dispositivo.

ACTUALIDAD LOPD

La Agencia y el Supervisor Europeo lanzan un documento que identifica los 10 errores más comunes sobre "*machine learning* y protección de datos"

Fuente: AEPD

(Madrid, 20 de septiembre de 2022). La Agencia Española de Protección de Datos (AEPD) y el Supervisor Europeo de Protección de Datos (EDPS) han publicado un nuevo documento conjunto en el que exponen los 10 malentendidos más comunes relacionados con el *machine learning* (aprendizaje automático) y aportan un análisis de cuál debería ser el enfoque correcto.

El objetivo de estos documentos (versión en español y en inglés) es dilucidar los conceptos erróneos más comunes que rodean a los sistemas de *machine learning*, además de subrayar la importancia de implementar estas tecnologías de acuerdo con los valores de la UE, los principios de protección de datos y el respeto a los derechos de las personas.

La UE ha identificado la inteligencia artificial (IA) como una de las tecnologías más relevantes del siglo XXI, y ha destacado su importancia en la estrategia para la transformación digital de la UE. Al tener una amplia gama de aplicaciones, la IA puede contribuir en áreas tan dispares como el tratamiento de enfermedades crónicas, la lucha contra el cambio climático o la anticipación de amenazas de ciberseguridad.

"Inteligencia artificial", sin embargo, es un término general que engloba a aquellas tecnologías que tienen como objetivo imitar las capacidades de razonamiento humano, que pueden tener aplicaciones y limitaciones muy diferentes. Con frecuencia, los proveedores de tecnología promocionan sus sistemas haciendo referencia a la IA y, sin especificar qué tipo de IA.

El aprendizaje automático (*Machine Learning* o *ML*) es una rama específica de la IA, aplicada a la resolución de problemas específicos y limitados, como tareas de clasificación o predicción. A diferencia de otros tipos de IA que intentan emular la experiencia humana (por ejemplo, sistemas expertos); el comportamiento de los sistemas de aprendizaje automático no está definido por un conjunto predeterminado de instrucciones.

Los modelos de *ML* se entrenan utilizando conjuntos de datos. Durante su entrenamiento, los sistemas de *ML* se adaptan de forma autónoma a los patrones encontrados en las diferentes variables de un conjunto de datos dado, creando correlaciones. Una vez entrenado, el sistema utilizará los patrones aprendidos para generar un resultado.

El objetivo de este documento es dilucidar los conceptos erróneos comunes que rodean a los sistemas de *ML*, al tiempo que subrayar la importancia de implementar estas tecnologías de acuerdo con los valores de la UE, los principios de protección de datos y el total respeto a las personas.

Puede ver más información en el siguiente enlace

10 MALENTENDIDOS SOBRE EL *MACHINE LEARNING* (APRENDIZAJE AUTOMÁTICO)

EL PROFESIONAL RESPONDE

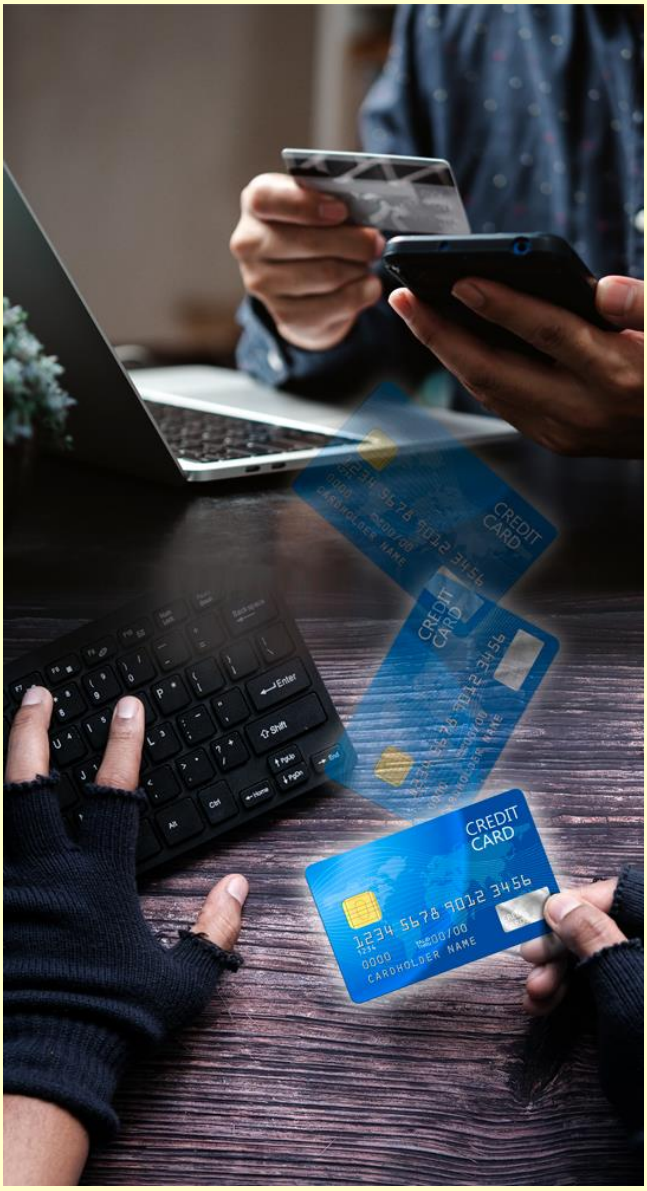
La seguridad en el comercio electrónico. Tipos de comercio electrónico (I)

La digitalización es un proceso que sigue en un imparable ascenso y aplica a todos los ámbitos de la vida. Con especial relevancia se han impuesto los medios electrónicos como medio de comunicación y consumo.

Hoy en día, son muchas las empresas que utilizan el comercio electrónico como principal método de negocio. Se conoce comúnmente como *e-commerce* en el cuál el pago lo realizamos mediante medios electrónicos.

En este boletín y siguientes vamos a definir los diferentes tipos de comercio electrónico en función de cómo se produce el intercambio entre el comprador y vendedor y las medidas de seguridad adecuadas para garantizar una venta segura.

- Tienda Online: realización de ventas a través de Internet.
- De afiliación: La venta, se realiza en una plataforma diferente a la tienda online. Esta plataforma se llevará una comisión de la venta.
- *Dropshipping*: el vendedor no envía el producto, lo hace un tercero.
- *Marketplace:* es una tienda que alberga a su vez varias tiendas.
- Membresía: compras recurrentes a través de suscripciones periódicas.
- Servicios: venta de servicios a través de Internet.



IMPORTANTE

Cada uno de los diferentes tipos de comercio electrónico deben garantizar una compraventa segura al consumidor.