Boletín 11/22

LOPD EN LA EMPRESA

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

Altabir consulting

www.altabir.es

EL RGPD UE 2016/679 EN APLICACIÓN

Roles en la protección de datos: el corresponsable del tratamiento

En la normativa de protección de datos encontramos regulada la figura del corresponsable del tratamiento en el artículo 26 del RGPD. **En este caso, cuando nos encontramos ante la situación de que dos o más responsables determinan de forma conjunta los objetivos y los medios de tratamiento serán considerados corresponsables.**

Lo más importante de esta figura es que las decisiones sobre el tratamiento de datos personales se determinan de forma transparente y de mutuo acuerdo. En particular, deberán definir los siguientes aspectos:

- Ejercicio de los derechos del interesado
- Deber de informar al interesado

La figura de la corresponsabilidad no tiene que estar presente en todo el tratamiento de datos personales, sino solamente en aquellas etapas del tratamiento en el que sea necesario determinar los fines y los medios conjuntamente.

Todos los aspectos relativos a protección de datos, tendrán que reflejarse en un acuerdo y este acuerdo deberá ponerse a disposición del interesado.

Contenido

1. Roles en la protección de datos: el corresponsable del tratamiento.
2. Empresa sancionada con 70.000 € por infringir la normativa de protección de datos.
3. Privacidad y seguridad en Internet: ¿tengo obligación de dar mis datos cuando me los piden?
4. Guía y Herramienta básica de anonimización.
5. La seguridad en el comercio electrónico: medidas de ciberseguridad. Protocolos de seguridad.

IMPORTANTE

Los interesados podrán ejercer los derechos ante cualquiera de los responsables que figuren en el acuerdo de corresponsabilidad.

SANCIONES DE LA AEPD

Empresa de reparto sancionada con 70.000 € por infringir la normativa de protección de datos

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00280-2022.pdf, se sanciona a una conocida empresa de reparto por haber actuado en contra de los principios de la normativa de protección de datos.

La reclamante manifestó en su escrito que se habían cedido datos personales sin su consentimiento, puesto que el paquete que deberían haberle entregado a ella al encontrarse ausente, se lo entregaron a una vecina de su comunidad sin que ella hubiera manifestado su consentimiento.

Ante esta reclamación, la empresa de mensajería alega que en los términos de su contrato se recoge la posibilidad de entrega al vecino si el receptor no estuviera disponible salvo que se excluya esta opción. Ante lo cual, el establecimiento online donde fue comprado el producto debería haber marcado esta excepción.

La AEPD dispone en su resolución que no se puede hacer responsable al establecimiento ya que no existía ninguna relación de encargado del tratamiento y por lo tanto el comercio online no tenía instrucciones de cómo realizar el tratamiento. Se le sanciona con **50.000 €** por infringir el art.5.1. f del RGPD ante la falta de confidencialidad y con **20.000 €** por no haber aplicado medidas de seguridad adecuadas que garantizasen la confidencialidad en el tratamiento de los datos.

Se considera una infracción grave la falta de diligencia en la aplicación de medidas de seguridad técnica y organizativas que minimicen los riesgos del tratamiento de los datos personales.

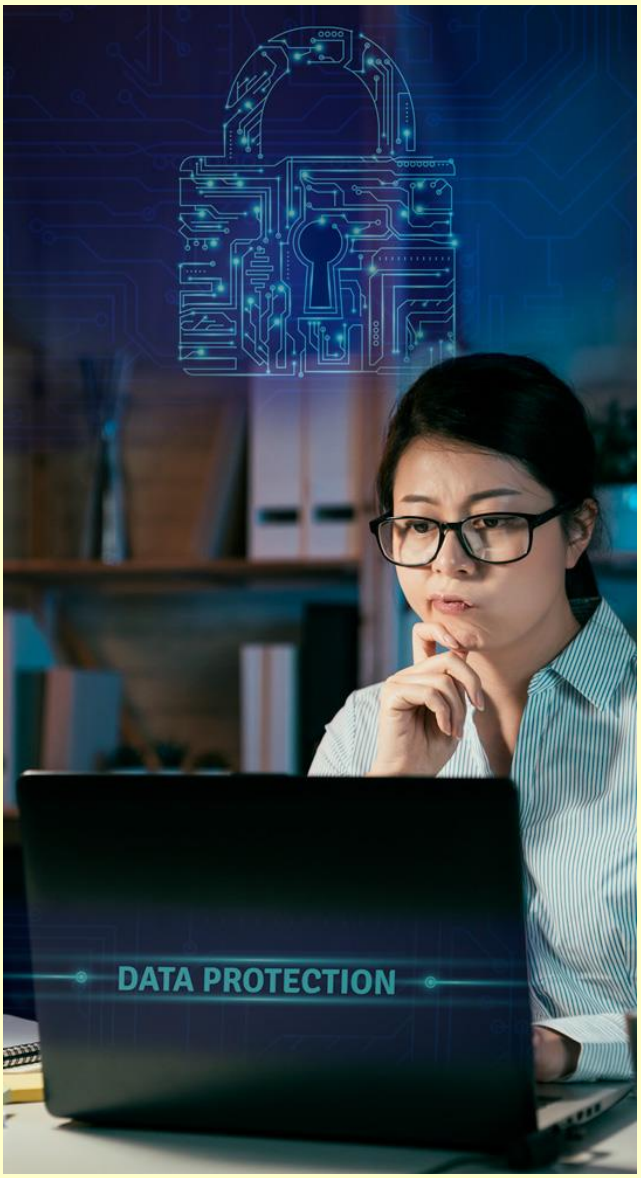
IMPORTANTE

El responsable del tratamiento debe aplicar medidas de seguridad técnicas y organizativas adecuadas para garantizar la confidencialidad de los datos.

LA AEPD ACLARA

Privacidad y seguridad en Internet: ¿tengo obligación de dar mis datos cuando me lo piden?

La privacidad y la seguridad en Internet, hoy en día, es un aspecto fundamental que ha de estar presente en el tratamiento de los datos personales. La AEPD junto con otros organismos, INCIBE (Instituto Nacional de Ciberseguridad) y OSI (Oficina de Seguridad del Internauta) en su guía de Privacidad y seguridad en Internet, **dan consejos y recomendaciones prácticas para proteger los datos personales y no dar más información de la necesaria:**



1. Antes de facilitar los datos personales se debe analizar quién es el responsable que los está pidiendo y la finalidad.
2. **Cualquier información que te identifique o pueda permitir que alguien lo haga es un dato personal, como, por ejemplo, nombre y apellido, correo electrónico o la dirección *IP.***
3. No se debe facilitar información personal de terceros, salvo que te hayan dado su consentimiento, o bien seas el tutor o representante legal.
4. **Dar más información de la necesaria puede resultar perjudicial, tu privacidad e identidad se pueden ver comprometidas.**
5. Podemos ser víctima de extorsión o chantaje cuando facilitamos información que no es necesaria para la finalidad del tratamiento.

Existen excepciones en los que no se requiere el consentimiento para el tratamiento de datos personales, tales como, para proteger intereses vitales y cuando exista una ley que lo habilite.

IMPORTANTE

El responsable del tratamiento debe facilitar la información sobre el tratamiento de los datos personales, entre otros, la finalidad, la cesión y el plazo de conservación de los datos.

ACTUALIDAD LOPD

Guía y Herramienta básica de anonimización

Fuente: AEPD

(Madrid, 2 de noviembre de 2022). La Agencia Española de Protección de Datos (AEPD) ha publicado la 'Guía básica de anonimización', un documento elaborado por la Autoridad Nacional de Protección de Datos de Singapur (PDPC) y que, en colaboración con dicha autoridad, se ha traducido por su **valor didáctico y especial interés** para responsables, encargados de tratamientos y delegados de protección de datos.

Esta guía tiene como objetivo proporcionar una introducción y orientación práctica a las organizaciones sin experiencia previa en anonimización para que tengan orientaciones sobre **cómo realizar anonimización básica y desidentificación de conjuntos de datos**.

El documento dedica un capítulo específico a explicar la diferencia entre los **conceptos de anonimización** –conversión de datos personales en datos que no puedan utilizarse para identificar a ningún individuo–; **desidentificación**, que consiste en la eliminación de identificadores (nombre, dirección, número de documento nacional de identidad, etc.) que identifican directamente a un individuo, y **reidentificación**, referida a la identificación de individuos a partir de un conjunto de datos que previamente fue desidentificado o anonimizado.

Asimismo, aborda los **conceptos básicos de anonimización**, como el propósito y utilidad de esta técnica, reversibilidad, características, información inferida o las herramientas disponibles en el mercado. Posteriormente, desglosa el **proceso de anonimización** en cinco pasos: Conozca sus datos; Desidentifique sus datos; Aplique técnicas de anonimización; Calcule su riesgo y Gestione sus riesgos. La guía se complementa con una herramienta gratuita (descargable a través de este enlace) para que las organizaciones puedan transformar conjuntos de datos simples aplicando técnicas de anonimización.

Finalmente, el documento repasa las principales **técnicas de anonimización** de datos, los atributos comunes de los datos y las técnicas de anonimización sugeridas, la k-anonimidad, la evaluación del riesgo de reidentificación y las herramientas de anonimización.

Estos recursos están especialmente orientados a servir a pymes y startups cuando se tienen que enfrentar a la anonimización de pequeños conjuntos de datos, y también a aquellos que se quieren introducir en los principios de anonimización.

Puede ver más información en el siguiente enlace

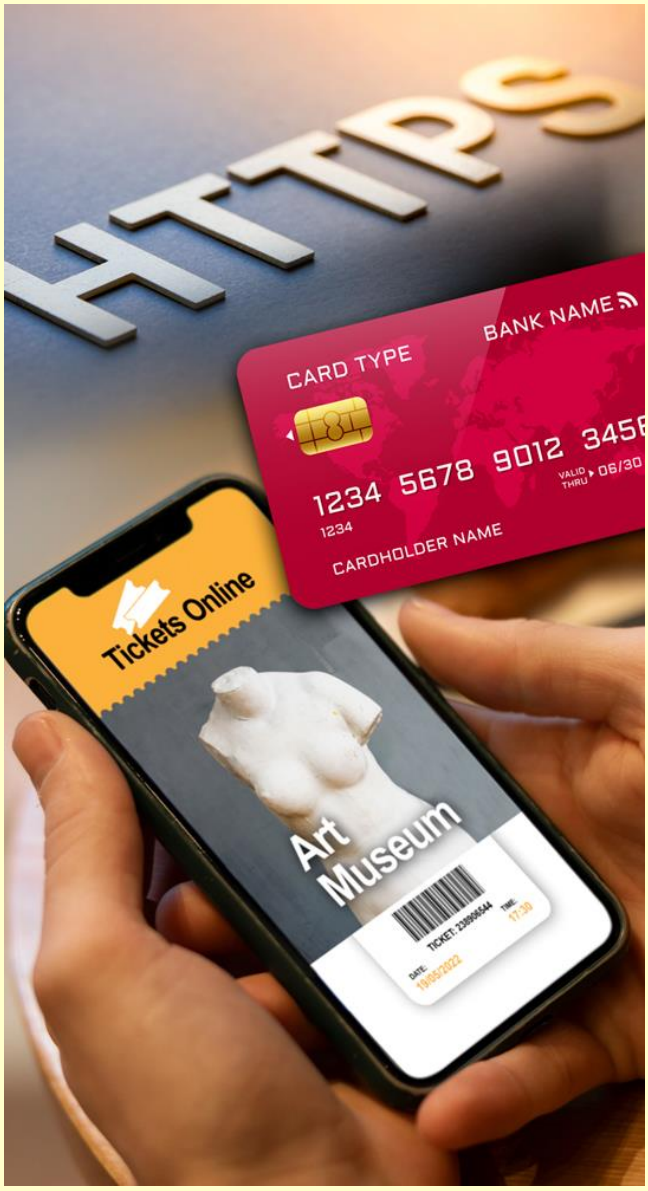
Guía básica de anonimización

Herramienta básica de anonimización

EL PROFESIONAL RESPONDE

La seguridad en el comercio electrónico: medidas de ciberseguridad. Protocolos de seguridad

La aplicación de medidas de ciberseguridad garantiza a nuestros clientes una compra segura. **Los principales protocolos para asegurar las transacciones en línea son:**



- **El protocolo *HTTPS*** *(Hyper Text Transfer Protocol Secure).* Se trata de un protocolo que incrementa el nivel de seguridad de las páginas web.
- **Los certificados *SSL*** *(Secure Sockets Layer)* garantizan la autentificación, confidencialidad e integridad de los datos. Para conseguirlo el navegador cifrará esos datos.
- **El protocolo *SET*** *(Secure Electronic Transaction).* En este caso, se requiere de la instalación de un software tanto por parte del vendedor como del comprador. Permite hacer una transacción segura con independencia del tipo de red utilizada en la conexión.

El proceso de pago es una de las operaciones más sensibles en el comercio electrónico, por lo que se recomienda la utilización del requerimiento del código *CVV (card verifictaion value)* de las tarjetas. Con este código nos garantizamos que el ciberdelincuente que solamente tenga el número de la tarjeta no pueda utilizarla de forma fraudulenta. Otro mecanismo de verificación recomendado es el que permite comprobar que la dirección de facturación coincide con la dirección archivada en el banco emisor de la tarjeta de crédito.

IMPORTANTE

Transmitir seguridad en el comercio electrónico garantiza el aumento de la cartera de clientes.