PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 04/22

EL RGPD UE 2016/679 EN APLICACIÓN

La importancia del registro de las actividades de tratamiento (I)

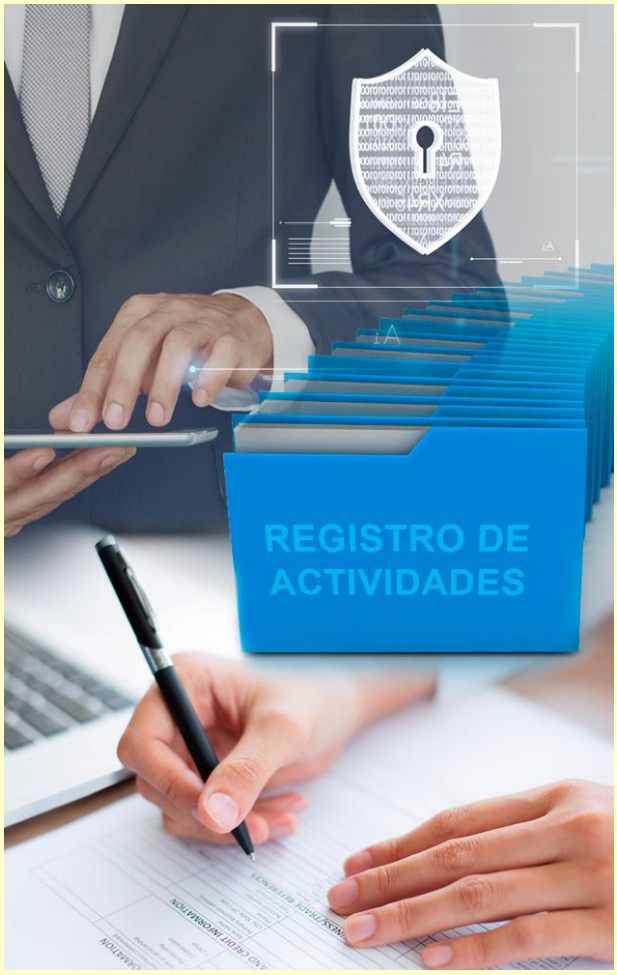
En primer lugar, acudimos a la definición que el RGPD hace de tratamiento como: ***"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no."***

Estas operaciones pueden ser, por ejemplo, la recogida de datos en un formulario de inscripción, la conservación de los datos en formato digital o papel para la finalidad por la cual se recogieron.

Todos los responsables y encargados de tratamiento tienen que realizar un registro de las actividades de tratamiento que efectúan bajo su responsabilidad. Este registro contendrá, entre otros:

- Nombre y datos de contacto del responsable y, en su caso, del corresponsable, representante y delegado de protección de datos.
- Fines del tratamiento.
- Categoría de interesados y datos personales.
- Categoría de destinatarios.
- Transferencias internacionales y sus garantías.
- Plazos previstos para la supresión de datos.
- Descripción general de las medidas de seguridad.

Contenido



IMPORTANTE

La LOPDGDD considera infracción grave no disponer del registro de actividades de tratamiento conforme a la normativa.

SANCIONES DE LA AEPD

Sancionado un Hotel con 30.000€ por utilizar la fotografía del pasaporte para el control de pagos

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00078-2021.pdf se sanciona a un hotel por utilizar la fotografía del pasaporte de los clientes para controlar los pagos que realiza el huésped durante su estancia.

El reclamante, un ciudadano holandés, interpuso la reclamación ante la Autoridad de control de Países Bajos, y se dio traslado a la AEPD, que actuó como autoridad de control principal. Aunque en un principio la autoridad española no encontró indicios de incumplimiento, la autoridad belga formuló objeciones al procedimiento, por lo que finalmente, la entidad reclamada fue sancionada.

El Hotel, en cumplimiento de la obligación de registro documental, tal y como se recoge en la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, tomaba los datos del huésped en el *check-in*. Además de los datos, escaneaban una copia del pasaporte que incluía la fotografía.

La autoridad de control sancionó al hotel por el uso posterior que se hace de esa fotografía. El hotel alegó que la fotografía servía de medio para evitar que se realizaran pagos fraudulentos con la tarjeta de crédito del cliente. A ella solo podía acceder el personal autorizado.

La autoridad de control entendió que el interés legítimo alegado para ese tratamiento no era el adecuado.

Los datos utilizados deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

IMPORTANTE

El responsable debe realizar un juicio de ponderación cuando alegue el interés legítimo para el tratamiento de datos personales.

LA AEPD ACLARA

Guía para la notificación de brechas de datos personales a la autoridad de control (I)

En el apartado de la AEPD Guías y Herramientas, encontramos el documento denominado Guía para la notificación de brechas de datos personales.

En esta guía se dan las indicaciones necesarias al responsable del tratamiento para notificar, en su caso, a la autoridad de control competente, las brechas de seguridad.

Si el incidente de seguridad, no afecta a datos personales o a tratamientos de datos personales, no se trataría de una brecha de datos. Tampoco se consideran brechas, cuando el tratamiento se lleve a cabo por personas físicas en el ámbito doméstico.

No es obligatorio notificar todas las brechas. El RGPD prevé una excepción cuando el responsable pueda garantizar que es improbable que la brecha de datos personales entrañe un riesgo.

Por otro lado, en la guía se hace referencia a que si lo que se pretende es denunciar por la posible vulneración de la normativa de un empleado, o tercero, el canal utilizado es el de presentación de reclamaciones.

El responsable del tratamiento es quién debe notificar a la autoridad de control. Aunque, este puede autorizar a una persona física, o representante. El encargado de tratamiento que ha sido objeto de la brecha, también podrá notificar a la autoridad de control siempre y cuando así venga establecido en el contrato.

En la sede electrónica encontramos el formulario en línea que permite hacer las notificaciones telemáticas.

IMPORTANTE

En todo tratamiento hay que determinar el riesgo que para los derechos y libertades puede suponer que se materialice una brecha de datos personales.

ACTUALIDAD LOPD

Las reclamaciones presentadas ante la AEPD aumentaron un 35% en 2021

Fuente: AEPD

(21 de marzo de 2022). La Agencia Española de Protección de Datos (AEPD) ha publicado hoy su Memoria 2021, que recoge de forma exhaustiva las actividades realizadas, las cifras de gestión, los informes y procedimientos más relevantes del año, y un análisis de los retos presentes y futuros. La actividad de organismo en 2021 ha estado centrada de forma prioritaria en una doble vertiente: **dar respuesta a los desafíos de protección de datos relacionados con la pandemia y seguir impulsando que aquellos que tratan datos** se comprometan con la protección de la privacidad. En el primer bloque, la Agencia ha continuado participando en articular garantías para proteger los datos personales en los tratamientos relacionados con las medidas contra la COVID-19, tanto en un plano nacional como en el europeo a través del Comité Europeo de Protección de Datos (CEPD). En el segundo, en 2021 se puso en marcha el Pacto Digital para la Protección de las Personas, una iniciativa que ya cuenta con casi 400 entidades adheridas y que promueve la privacidad y la ética digital como un activo que las organizaciones deben tener en cuenta a la hora de diseñar sus políticas y sus estrategias.
En cuanto a las cifras de gestión, en 2021 se han presentado ante la Agencia **13.905 reclamaciones, un aumento de un 35% respecto a 2020. Esta cifra asciende a las 14.571** incluyendo los casos transfronterizos, los casos en los que la Agencia actúa por iniciativa propia y las quiebras de seguridad trasladadas a inspección. En 2021 las **reclamaciones resueltas han aumentado un 35% (14.098**) respecto al año anterior (10.443), una cifra muy destacable que ha permitido resolver reclamaciones pendientes de ejercicios anteriores sin que hayan aumentado significativamente los tiempos medios de resolución. En esos tiempos de tramitación de las reclamaciones hay que hacer una referencia a los **traslados**, una previsión recogida por la LOPDGDD para facilitar la resolución rápida de las reclamaciones y que ha permitido que estas se resuelvan en menos de dos meses. (…)

En cuanto a las reclamaciones ordinarias, las **planteadas con mayor frecuencia** por los ciudadanos en 2021 corresponden a servicios de internet (16%), videovigilancia (12%), recepción de publicidad (excepto spam) (11%) e inserción indebida en ficheros de morosidad (9%). En cuanto a los procedimientos sancionadores, se finalizaron 585, un 49% más que en 2021. Las áreas más frecuentes en los procedimientos sancionadores son videovigilancia (25%), servicios de internet (22%), y publicidad a través de correo electrónico o teléfono móvil (9%).

Se han realizado 264 resoluciones que han finalizado con la imposición de multa. Las seis **áreas de actividad con mayor importe global de multas** han sido la publicidad (8.659.200 euros), telecomunicaciones (6.500.000 euros), entidades financieras/ acreedoras (6.243.000 euros), ficheros de morosidad (4.209.000 euros), contratación fraudulenta (3.674.000 euros) y asuntos laborales (2.625.900 euros).

Puede ver más información en el siguiente enlace

Memoria 2021

EL PROFESIONAL RESPONDE

Garantizar la seguridad de la información: seguridad en redes wifi (I)

Existen muchos tipos de redes inalámbricas, dependiendo de la arquitectura, tecnología o estándares de comunicación. En este blog nos referiremos a las Redes de Área Local inalámbricas (WLAN).

Los componentes de la red wifi son los denominados dispositivos cliente, que solicitan la conexión a la red inalámbrica. Pueden ser, por ejemplo, las *tablets*, los ordenadores portátiles, etc. **Y los puntos de acceso, (conocido como *router*)** que sirven como puertas de enlace a otras y conecta los dispositivos clientes entre ellos.

Dependiendo de la forma en que se intercambien los datos en la red, esta puede ser de dos tipos:

- Mod Ad Hoc, en este caso, no existen puntos de acceso. Los dispositivos se comunican entre sí, por ejemplo, a través de tecnologías como bluetooth.
- Mod infraestructura, es la que utilizamos normalmente en las casas y empresas. El punto de acceso (*router*) es el que nos conecta con otros dispositivos, impresoras, servidores, etc.

La utilización de este tipo de redes inalámbricas nos permite tener una gran movilidad y, a varios usuarios conectándose a la vez desde cualquier lugar donde llegue la señal. Además, no habrá que preocuparse del mantenimiento del cableado.

IMPORTANTE

La utilización de este tipo de redes conlleva la realización de un pormenorizado análisis de riesgos para mitigar los riesgos inherentes a estas redes wifi.