PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 09/22

EL RGPD UE 2016/679 EN APLICACIÓN

Roles en la protección de datos: el responsable de tratamiento

Contenido

En los siguientes boletines vamos a ir tratando los diferentes roles que operan en el tratamiento de los datos personales. **En la normativa en protección de datos, se regulan tres figuras que son; el responsable del tratamiento, el encargado del tratamiento y el corresponsable.** A estas tres, además, tenemos que sumar una figura fundamental, a resultas del carácter proactivo de la norma, este es el delegado de protección de datos.

Es importante diferenciar cada una de ellas. En el artículo 4 del RGPD, se define al responsable, como *"aquella persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medio del tratamiento"*. **Es decir, el responsable, es el que decide sobre determinados aspectos esenciales del tratamiento de los datos.** Preguntarnos acerca de por qué tiene lugar el tratamiento y quién ha decidido que debe llevarse a cabo el tratamiento para ese fin concreto, ayuda a definir el rol del responsable.

El responsable siempre decide sobre los fines del tratamiento. En cambio, respecto de los medios, podemos diferenciar entre medios esenciales y no esenciales. En los no esenciales puede decidir el encargado del tratamiento.

IMPORTANTE

Para ser considerado responsable no es necesario disponer de un acceso real a los datos que esté tratando.

SANCIONES DE LA AEPD

Una Comunidad de Propietarios es sancionada con 6.000€ por incumplir la normativa de protección de datos

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00523-2021.pdf, se sanciona con 6.000€ a una Comunidad de propietarios por el incumplimiento de varios preceptos de la normativa de protección de datos.

La reclamación es interpuesta por una propietaria de la comunidad. En su escrito manifestó, que, durante el verano del 2020, para entrar en la piscina comunitaria, le exigían que mostrara su DNI, el cuál era apuntado por el vigilante contratado, en un papel en blanco, a la vista del resto de usuarios de la piscina. La reclamante se puso en contacto con el presidente de la comunidad, el cual, le comunicó que se recogía ese dato por la situación de pandemia COVID-19 para facilitarlo al Ministerio de Sanidad en caso de brote. Esa decisión fue tomada solamente, en Junta directiva, pero no vecinal, tal y como manifestó la administradora de fincas.

La AEPD, en su fase de investigación, envío escrito de notificación a la Comunidad de propietarios para que enviara alegaciones, pero no presentó nada al respecto. **Se sanciona a la Comunidad con 6.000€ por excederse en el tratamiento de los datos, ya que, con apuntar el piso y letra hubiera sido suficiente para identificar al usuario de la piscina.** Además, también, se le sanciona por no informar debidamente del tratamiento de los datos personales.

La falta de información a los interesados/as en el tratamiento de sus datos supone una falta muy grave en nuestro ordenamiento jurídico.

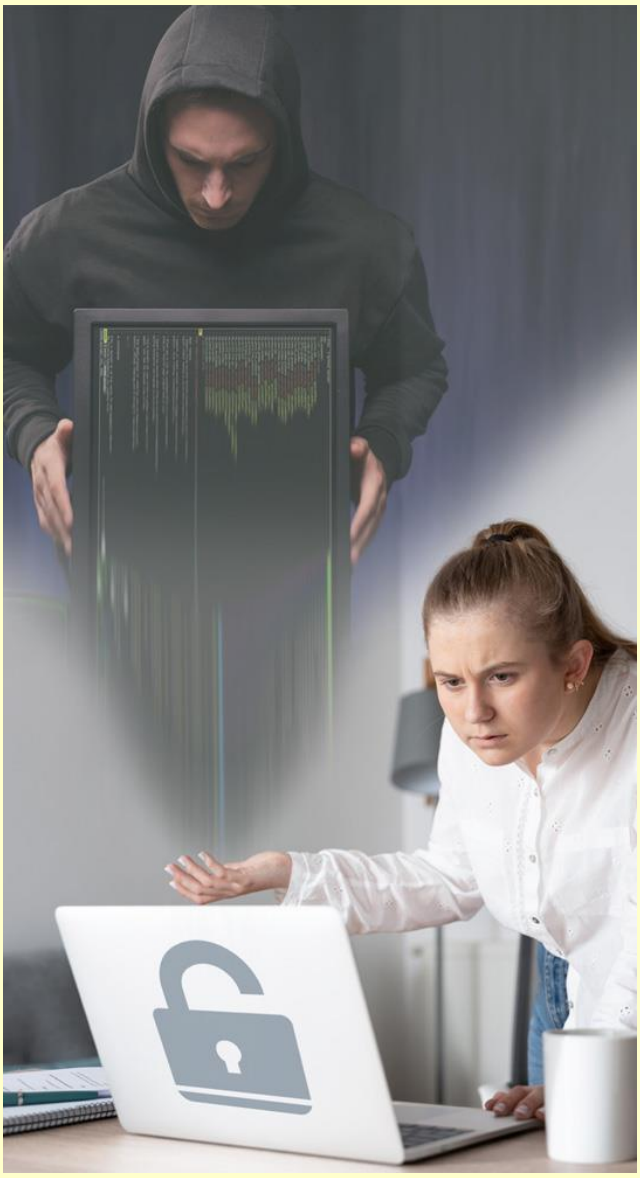
IMPORTANTE

Los datos personales tienen que ser los adecuados, pertinentes y limitados a lo necesario en relación con los fines del tratamiento.

LA AEPD ACLARA

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

La Unidad de Evaluación y Estudios Tecnológicos de la AEPD, editó unas recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo. Estas recomendaciones están dirigidas a responsables del tratamiento y al personal que participa en las operaciones de tratamiento.



Las recomendaciones para el responsable son:

1º Definir una política de protección de la información para situaciones de movilidad. Entre otros aspectos, se determinarán que formas de acceso remoto se permiten, qué tipo de dispositivos son válidos para cada forma de acceso y el nivel de acceso permitido en función de los perfiles. Se informará al usuario de las amenazas en que pueden verse afectados al trabajar fuera de la organización.

2º Elegir soluciones y prestadores de servicio confiables y con garantías. Cuando accedan a datos de carácter personal, tendrán la consideración de encargados de tratamiento que se regirá por un contrato de acceso a datos.

3º Restringir el acceso a la información. Dependiendo de los perfiles o niveles de acceso a los recursos y a la información.

4º Configurar periódicamente los equipos y dispositivos utilizados en situaciones de movilidad.

5º Monitorizar los accesos realizados a la red corporativa desde el exterior.

IMPORTANTE

En la política de protección de la información para situaciones de movilidad se informará sobre el alcance de las actividades de control y supervisión.

ACTUALIDAD LOPD

Empleo de datos biométricos: evaluación desde la perspectiva de protección de datos

Fuente: AEPD

Los tratamientos que incluyen operaciones con datos biométricos se pueden emplear con muchas finalidades: prueba de vida, identificación, autenticación, seguimiento, perfilado, decisiones automáticas, etc. Las operaciones biométricas pueden emplear distintas técnicas, algunas de forma simultánea, y, a su vez, una misma técnica se puede implementar de formas diferentes. Las operaciones con datos biométricos en un tratamiento concreto tendrán un grado distinto de intrusión e impacto en la privacidad de los individuos que dependerá de la técnica empleada, pero también de la propia definición del tratamiento, su naturaleza, el ámbito o alcance en el que se va a desarrollar, su contexto y, en especial, los fines que se persiguen. Por lo tanto, la evaluación de impacto de las operaciones biométricas se ha de realizar en el marco de un tratamiento y con relación a sus fines últimos.

Las técnicas de proceso de datos biométricos se basan en recoger y procesar rasgos físicos, conductuales, fisiológicos o neuronales de las personas mediante dispositivos o sensores, creando firmas o patrones que posibilitan la identificación, seguimiento o perfilado de las personas. Algunos métodos requieren la cooperación de la persona, mientras que otros métodos pueden capturar datos biométricos a distancia, sin requerir la cooperación del individuo y sin que pueda tener conciencia de ello.

En el marco de un tratamiento, cualquiera de las distintas técnicas biométricas que se incluyan tienen que ser evaluadas de acuerdo con la adecuación, proporcionalidad y la necesidad, su finalidad, su el impacto en los derechos y libertades de las personas físicas y los riesgos que conllevan, tanto para el individuo como para la sociedad.

Existen distintos criterios de clasificación de los sistemas biométricos: algunos basados en el uso de tecnologías diferentes, otros relacionados con los dispositivos o sensores, otros con relación al rasgo o conjuntos de rasgos estudiados, etc. Sin embargo, a la hora de demostrar la adecuación de un tratamiento al Reglamento General de Protección de Datos (RGPD), y de evaluar el riesgo para los derechos y libertades de los individuos que puede suponer el procesamiento de dichos datos, es conveniente emplear criterios de clasificación de las operaciones biométricas desde el punto de vista de protección de datos y con relación al tratamiento en el que se implementa.

La validación de las técnicas biométricas empleadas en un tratamiento ha de realizarse “desde el diseño” tal y como exige el artículo 25.1 del RGPD y con las recomendaciones que establece en la Guía de Privacidad desde el Diseño. El análisis de estos factores, y otros que puedan ser específicos del tratamiento o de la operación biométrica elegida, permitirán realizar un análisis del cumplimiento normativo, de la necesidad y proporcionalidad del tratamiento permitiendo una gestión del riesgo más adecuada.

Puede ver más información en el siguiente enlace

Nota técnica: 14 equívocos con relación a la identificación y autenticación biométrica

EL PROFESIONAL RESPONDE

La seguridad en la nube: amenazas y riegos (II)

La gestión de las amenazas y riesgos que conlleva la utilización de los servicios *cloud,* resulta imprescindible para mantener el control sobre la información y garantizar su protección y disponibilidad en cualquier momento. Vamos a enumerar las principales amenazas, riesgos y su mitigación.

Entre las amenazas podemos destacar las amenazas internas de empleados/as insatisfechos o exempleados/as que pueden provocar situaciones de riesgo cuando no se gestionan los permisos y privilegios de acceso. El problema del uso de las tecnologías compartidas puede provocar que por un fallo de seguridad usuarios de otras empresas accedan a nuestra información. La suplantación de identidad, es otra de las amenazas, cuando los ciberdelincuentes por ingeniería social se hacen con las credenciales de algún usuario.

Un análisis de riesgos adecuado a la empresa, nos garantiza una gestión del riesgo que permita mitigarlo. Por ejemplo, ante el riesgo de falta de aislamiento de los datos, para gestionar su mitigación, los datos en reposo deben estar aislados y los procedimientos de cifrado ejecutados por personal formado. La empresa debe saber dónde está localizada la información más sensible y adoptar medidas de protección. Otro ejemplo, para evitar la indisponibilidad del servicio, hay que exigir a los proveedores una óptima capacidad de recuperación de datos y el tiempo estimado.

IMPORTANTE

Para reducir los riesgos en la nube se tiene que aplicar el mismo concepto de seguridad que se exige en las instalaciones físicas.