PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 06/21

EL RGPD UE 2016/679 EN APLICACIÓN

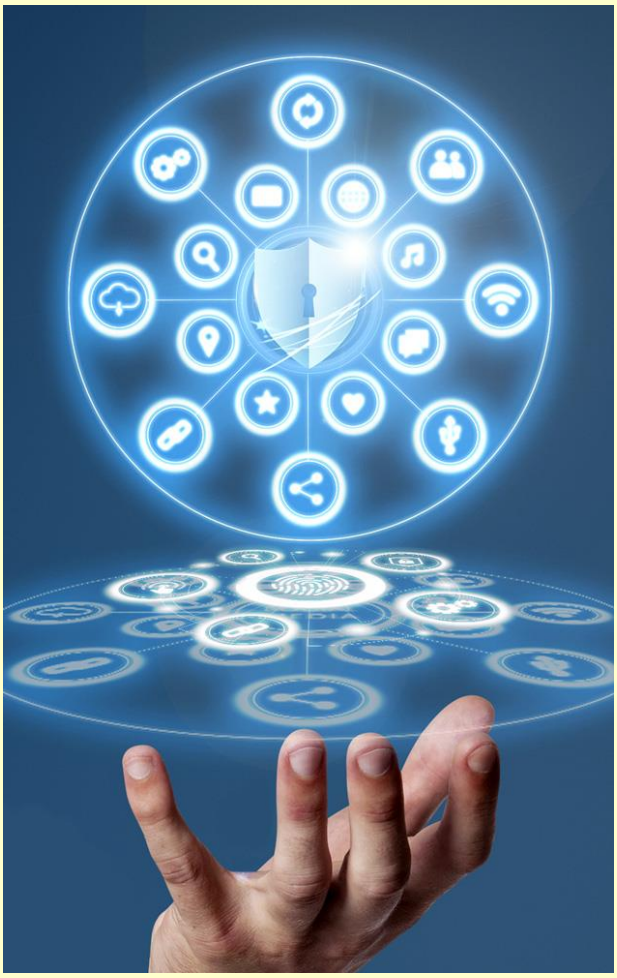
Principales funciones del Delegado de Protección datos

El Delegado de Protección de datos, dentro de una empresa, tiene que ser designado atendiendo sus cualidades profesionales, en particular tal y como nos dice el RGPD, ha de tener conocimientos especializados del Derecho y práctica en la materia de protección de datos para poder desempeñar con éxito las funciones que tiene encomendadas.

¿Cuáles son sus principales funciones?

- **Informar y asesorar al responsable o encargado del tratamiento y a los empleados** que se ocupen del tratamiento de las obligaciones contenidas en el RGPD y en nuestra LOPDPGDD
- **Supervisar el cumplimiento de la normativa de protección de datos en las actividades** realizadas por la empresa.
- **Supervisar las políticas de protección de datos, incluyendo la asignación de responsabilidades, la concienciación y formación del personal** en protección de datos.
- Verificar las auditorías correspondientes.
- Ofrecer asesoramiento en la evaluación de impacto y su verificación.
- **Cooperar y actuar como punto de contacto con la autoridad de control.**

Contenido



IMPORTANTE

Las Autoridades de control podrán remitir al Delegado de Protección de datos las reclamaciones interpuestas por los ciudadanos

SANCIONES DE LA AEPD

Sancionada con 4.000€ una asesoría por comunicar datos de un cliente a otra asesoría sin su consentimiento

En la Resolución de la AEPD https://www.aepd.es/es/documento/ps-00116-2021.pdf , se sanciona a una asesoría fiscal por no haber solicitado el consentimiento de la afectada.

La AEPD es una de las Autoridades de Control Europeas que gestiona mayor número de expedientes sancionadores

La reclamante manifiesta en su escrito de reclamación que sus datos fueron comunicados por su asesoría fiscal a otra asesoría, de la cuál recibió una factura a su cargo por los servicios prestados. En ningún momento se pusieron en contacto con ella para solicitarle el consentimiento del tratamiento de sus datos.

La Subdirección General de Inspección de datos inició el proceso de investigación, solicitando información sobre las causas. No se obtiene ninguna contestación sobre las mismas, lo que supone un agravante a tener en cuenta en el momento de cuantificar la sanción, puesto que una de las obligaciones del responsable es colaborar con la autoridad de control cuando ésta se lo requiera.

Se ha vulnerado el art. 6 del RGPD que recoge los supuestos de licitud del tratamiento por parte de terceros. En este caso, la asesoría fiscal con la que tenía contratado sus servicios comunica los datos a un tercero sin su consentimiento, por lo que no está actuado diligentemente.

La cuantía finalmente reclamada ascendió a 4.000€, teniendo en cuenta el agravante de la nula cooperación con la AEPD con el fin de poner remedio a la infracción y mitigar sus efectos.

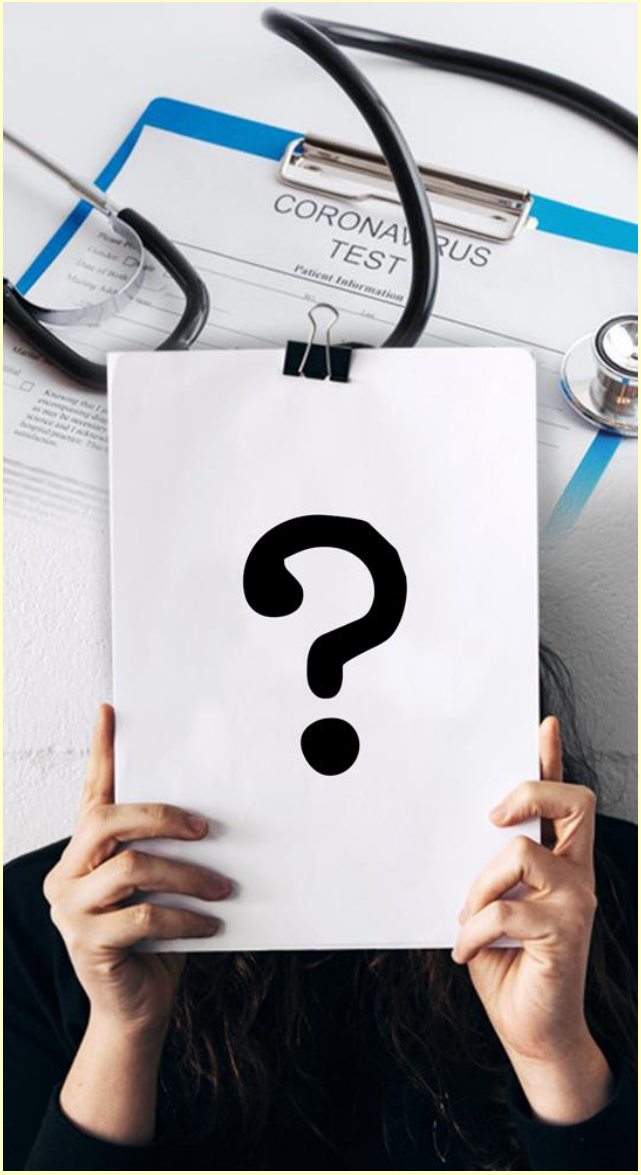
IMPORTANTE

La sanción podría haberse evitado si la empresa hubiera tenido un protocolo de actuación en materia de protección de datos.

LA AEPD ACLARA

10 malentendidos relacionados con la anonimización

La AEPD ha publicado una miniguía **ilustrando los 10 principales malentendidos relacionados con la anonimización.** Los datos anónimos son aquellos datos que no hacen referencia a personas naturales identificadas o identificables. Hoy en día tienen un papel importante en el contexto de la investigación en áreas como la medicina, marketing, economía, y muchas otras.



1º La seudonimización es lo mismo que anonimización. No es así, los datos anónimos no pueden asociarse a un individuo en particular, mientras que en la seudonimización con una información adicional identificaríamos a la persona.

2º El cifrado es anonimización. No es una herramienta válida.

3º Los datos siempre pueden anonimizarse. No siempre es posible reducir el riesgo de reidentificación y que los datos sean válidos.

4º La anonimización es permanente. Existe un riesgo de que ciertos procesos se reviertan en el futuro.

5º Siempre se consigue reidentificación cero.

6º Es un concepto binario que no puede medirse.

7º Se puede automatizar totalmente.

8º Se inutilizan los datos.

9º Seguir procesos de anonimización de otros.

10º No existe riesgo ni interés en saber a quién se atribuyen esos datos.

IMPORTANTE

El objetivo de la anonimización es evitar que se identifique a los individuos de un conjunto de datos. Su utilidad dependerá de la finalidad y del riesgo aceptado

ACTUALIDAD LOPD

La AEPD publica una nueva version de su guía para notificar brechas de datos personales

Fuente: AEPD

(Madrid, 25 de mayo de 2021). La Agencia Española de Protección de Datos (AEPD) ha publicado hoy una actualización de su 'Guía para la notificación de brechas de datos personales', un documento que tiene como objetivo **guiar a los responsables de los tratamientos de datos personales** en su obligación de notificarlas a las autoridades de protección de datos y comunicárselo a las personas cuyos datos se hayan visto afectados. Esta guía actualiza la versión publicada en 2018, cuando comenzó a aplicarse el Reglamento General de Protección de Datos (RGPD), e incluye la experiencia recogida en este tiempo, tanto a nivel nacional como en relación con los criterios establecidos por el Comité Europeo de Protección de Datos.

El principal propósito de esta actualización es facilitar el cumplimiento de forma eficaz y eficiente de los objetivos últimos de la notificación de brechas de datos personales: **la protección efectiva de los derechos y libertades de las personas**, la creación de un entorno más resiliente basado en el conocimiento de las vulnerabilidades de la organización y la garantía de una seguridad jurídica al disponer los responsables de un medio para demostrar diligencia en el cumplimiento de sus obligaciones.

Cualquier organización se encuentra expuesta a sufrir una brecha de datos personales que pueda repercutir en los derechos y libertades de las personas, y **está obligada a gestionarla de forma adecuada**. Este incidente puede tener un origen accidental o intencionado y, generalmente, ocasiona la destrucción, pérdida, alteración, comunicación o el acceso no autorizado a datos personales. La Guía comienza analizando qué es una brecha de datos personales y qué no lo es en el contexto del marco normativo europeo, nacional y sectorial. A continuación analiza cuándo hay que notificar dicha brecha a la autoridad de control, en qué plazo, o quién y qué contenido debe incluir esa notificación. En lo relativo a la comunicación a las personas afectadas, el documento recoge en qué casos hay que realizarla, el contenido y sus plazos.

Las notificaciones y comunicaciones relativas a brechas que afectan a datos personales forman parte de la **responsabilidad proactiva** establecida en el RGPD, y el hecho de notificarla o comunicarla no implica necesariamente la imposición de una sanción. De hecho, hacerlo en tiempo y forma es una evidencia de la diligencia de la organización, mientras que no cumplir con esa obligación sí está tipificado como infracción. La Guía ofrece directrices para facilitar y simplificar el cumplimiento de estas obligaciones y, entre otros puntos, orienta sobre algunos plazos que el RGPD deja abiertos.

Puede ver más información en el siguiente enlace

Guía para la notificación de brechas de datos personales

EL PROFESIONAL RESPONDE

Ransomware, la principal amenaza para las empresas (I)

Hemos visto como en la actualidad muchas empresas han sido objeto de ciberataques a través de ransomware. El tamaño de la empresa es independiente para los ciberdelincuentes y cualquier entidad puede ser objetivo de un ataque informático.

¿Qué es un ransomware? Se trata de un tipo de malware que está en continua evolución y que impide el acceso a la información de un dispositivo, amenazando con destruirla o hacerla pública si las víctimas no acceden a pagar un rescate en un tiempo determinado.

¿Cómo puede llegar a nuestra empresa?

Se puede propagar de distintas maneras;

- A través de campañas de Spam
- Por la existencia de vulnerabilidades o malas configuraciones de software
- Actualizaciones de software falsas
- Utilización de canales de descarga de software no confiables
- Instalación de herramientas de activación de programas no oficiales.

Lo que se pretende es que la víctima abra un archivo adjunto infectado o haga clic en un vínculo que le lleve al sitio web del atacante, donde será infectado.

Con este tipo de ataques, además de bloquear la información y exigir un rescate, se amenaza con la fuga de información confidencial al ámbito público (internet), lo que ocasionaría sanciones a la empresa por incumplimiento del RGPD.

IMPORTANTE

El rescate se suele solicitar a través de criptodividas. Se recomienda no pagar el rescate para evitar la proliferación de este tipo de amenazas