PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 06/22

EL RGPD UE 2016/679 EN APLICACIÓN

Tratamientos concretos: Sistema de denuncias internas

En nuestra Ley orgánica LOPDGDD se regula el tratamiento concreto del sistema de denuncias internas. **Este sistema permite poner en conocimiento de una entidad, incluso de forma anónima, la comisión de actos o conductas que puedan resultar contrarias a la normativa general o sectorial, ocurridos en la propia entidad, o bien, en la actuación con terceros que contraten con ella.**

En el art. 24 de la LOPDGDD se regulan aspectos concretos del sistema de denuncias interna. Señalamos a continuación alguno de ellos:

- La licitud del tratamiento proviene de la existencia de un interés público.
- Los empleados y terceros deben ser informados de la existencia del sistema.
- El acceso se limita a los que tienen funciones de control interno y cumplimiento.
- Deben adoptarse medidas necesarias para preservar la identidad y confidencialidad.
- Los datos se conservarán durante el tiempo necesario para decidir si se inicia una investigación. A los tres meses se suprimirán.
- Transcurrido el plazo anterior, los datos se tratarán por el órgano correspondiente, para la investigación de los hechos.

Contenido

IMPORTANTE

El Ministerio de Justicia ha aprobado el anteproyecto de Ley que regulará la creación de los sistemas y los derechos y garantías del informante.

SANCIONES DE LA AEPD

Multan a un restaurante por publicar el nombre y apellidos de una extrabajadora en las reseñas de Google

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00395-2021.pdf se sanciona a un restaurante por la publicación de los datos personales de una extrabajadora en las reseñas de Google.

La reclamante denunció ante la AEPD la publicación de sus datos personales en Internet. Manifiesta que el propietario del restaurante en el que trabajaba respondió a las reseñas negativas que habían publicado en Google, alegando que las criticas venían de parte de los amigos de la reclamante, y para ello, identificó a la extrabajadora con nombre y apellidos, revelando, además, las circunstancias de su sanción laboral.

Junto a la reclamación, aporta cuatro capturas de pantalla, con el título *"Respuesta del propietario",* en las que se visualiza la contestación a diferentes reseñas, en las cuáles, incluye el nombre y apellidos de la reclamante.

La Subdirección General de Inspección procedió a la realización de actuaciones previas de investigación, solicitando información a la entidad reclamada, sin obtener respuesta alguna por parte de esta. **Finalmente, la AEPD, a la vista de los hechos, le impuso una sanción de 1.500 €** por la infracción del art.5.1. f, falta de confidencialidad y el art.6.1.a el tratamiento es ilícito por la publicación sin el consentimiento.

Son sanciones consideradas muy graves, la vulneración del deber de confidencialidad.

IMPORTANTE

La publicación de datos de terceros en Internet requiere del consentimiento del interesado afectado, salvo que, esté exceptuado legalmente.

LA AEPD ACLARA

El nombramiento y funciones del Delegado de Protección de Datos

El Gabinete jurídico de la AEPD publicó un informe sobre las funciones y nombramiento del delegado de protección de datos.

La AEPD ha ido señalando de forma reiterada el papel fundamental que dentro del modelo de responsabilidad activa desempeña el delegado de protección de datos. Su nombramiento no se debe interpretar solamente como una formalidad, sino que, se tendrán que aplicar todos los requisitos que se recogen en la normativa aplicable.

Uno de estos requisitos, es la asignación de funciones, que como mínimo serán las recogidas en la norma, entre las que se encuentran, las funciones de asesoramiento y supervisión dirigidas a garantizar un adecuado cumplimiento de la normativa de protección de datos. **Por su parte, tanto el responsable como el encargado del tratamiento, establecerán los medios necesarios para que el delegado de protección de datos pueda participar de forma adecuada y en tiempo oportuno de las cuestiones relativas a la protección de datos personales.**

En cuanto a los requisitos de capacitación, el RGPD dispone que el delegado de protección de datos será designado atendiendo a sus cualidades profesionales, y en particular, a los conocimientos especializados que tenga del Derecho y la práctica en materia de protección de datos, así como su capacidad para desempeñar las funciones que la normativa de protección de datos le asigne.

IMPORTANTE

La cualificación del delegado de protección de datos podrá demostrarse a través de mecanismos de certificación.

ACTUALIDAD LOPD

La AEPD sanciona a Google LLC por ceder datos a terceros sin legitimación y obstaculizar el derecho de supresión

Fuente: AEPD

(18 de mayo de 2022). La Agencia Española de Protección de Datos (AEPD) ha dictado resolución del procedimiento iniciado contra la compañía Google LLC en la que declara la existencia de **dos infracciones muy graves** de la normativa de protección de datos e impone una sanción de **10 millones de euros** por ceder datos a terceros sin legitimación para ello y obstaculizar el derecho de supresión de los ciudadanos (artículos 6 y 17 del Reglamento General de Protección de Datos).

Google LLC es la responsable del tratamiento analizado y lo lleva a cabo en EEUU. En el caso de la **comunicación de datos a terceros**, la Agencia ha constatado que Google LLC envía al Proyecto Lumen información de solicitudes que le realizan los ciudadanos, incluida su identificación, dirección de correo electrónico, los motivos alegados y la URL reclamada. La misión de ese proyecto es la recogida y puesta a disposición de solicitudes de retirada de contenido, por lo que la Agencia considera que, dado que se remite toda la información contenida en la solicitud del ciudadano para que se incluya en otra base de datos accesible al público y para que se divulgue a través de una web, "supone en la práctica frustrar la finalidad del ejercicio del derecho de supresión".

La resolución recoge que esta comunicación de datos por parte de Google LLC al Proyecto Lumen se impone al usuario que pretenda utilizar sus formularios, **sin opción de oponerse** a la misma y, por tanto, sin que exista un consentimiento válido para que esa comunicación se lleve a cabo. Establecer esta condición en el ejercicio de un derecho reconocido a los interesados no está amparado por el Reglamento General de Protección de Datos al generarse "un tratamiento adicional de los datos sobre los que versa la solicitud de supresión al comunicarlos a un tercero". Además, en la política de privacidad de Google LLC, no se hace mención a este tratamiento de datos personales de los usuarios, y tampoco aparece entre las finalidades la comunicación al Proyecto Lumen.

La AEPD también recoge en su resolución que, presentada la solicitud de retirada de contenido y atendido el derecho, es decir, acordada la supresión de los datos personales, "no cabe un tratamiento posterior de los mismos, como es la comunicación que Google LLC realiza al Proyecto Lumen".

En cuanto al ejercicio de derechos de los ciudadanos, la AEPD detalla en su resolución que "es difícil deducir si la solicitud se formula invocando la normativa de protección de datos personales, sencillamente porque esta normativa no se menciona en ninguno de los formularios, con independencia del motivo que el interesado seleccione de entre las opciones propuestas, salvo en el formulario denominado 'Retirada en virtud de la ley de privacidad de la UE', el único disponible que contiene una referencia expresa a esta normativa".

Puede ver más información en el siguiente enlace

Expediente N.º: PS/00140/2020

EL PROFESIONAL RESPONDE

Seguridad en el correo electrónico corporativo: Política de seguridad (I)

El correo electrónico es una herramienta de comunicación corporativa que facilita y agiliza el funcionamiento en una empresa**. A pesar de sus grandes beneficios como la accesibilidad, rapidez y la posibilidad de adjuntar archivos, se hace necesario definir un uso correcto y seguro.** En algunas ocasiones, los empleados/as pueden enviar documentos confidenciales a quien no debían por error, o bien desvelar la dirección de correo electrónico de clientes o usuarios. **En este sentido es muy importante concienciar al personal, a los usuarios/as del correo corporativo de las amenazas y dotarles de las herramientas adecuadas para que hagan un uso seguro del correo.**

La entidad debería elaborar unas Políticas de seguridad, en concreto, para el uso del correo electrónico**. Estas Políticas como mínimo tendrían que contener:**

- Normativa de uso de correo electrónico.
- Instalar aplicaciones antimalware y antispam.
- Instalar tecnología de cifrado y firma digital.
- Desactivar el formato HTML, ejecución de macros y descarga de imágenes.
- Contraseña segura. Elaboradas conforme a la Política de contraseñas.
- Identificación de correos sospechosos.
- Normas para evitar el uso de las redes públicas.

IMPORTANTE

Una utilización segura del correo electrónico corporativo evitaría caer en las trampas de los ciberdelincuentes.