PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 03/21

EL RGPD UE 2016/679 EN APLICACIÓN

# Informar de las garantías en las transferencias internacionales

**Uno de los principios fundamentales que el responsable de una empresa tiene que cumplir es la transparencia de la información en el tratamiento de los datos personales.**

Este principio está relacionado con el derecho del interesado a obtener toda la información que sea relevante en relación con sus datos personales.

En los artículos 13 y 14 del RGPD se recogen todos los puntos que el responsable debe facilitar cuando trata datos personales. Además de indicar la identidad y datos de contacto del responsable, en su caso, del delegado de protección de datos, los fines del tratamiento y los destinatarios, **el responsable está obligado también a informar de su intención de realizar transferencias internacionales de datos.**

**En el caso de que las transferencias estén basadas en garantías adecuadas, normas corporativas vinculantes o en los supuestos de las excepciones para situaciones específicas se tiene que dejar indicado lo siguiente:**

- Copia de las garantías adecuadas
- Lugar en el que se hayan puesto a disposición, es decir, se ha de incluir en la información, una URL que permita al interesado acceder al documento que contiene dichas garantías.

## Contenido




**IMPORTANTE**

Se debe de poner a disposición del interesado el documento de las garantías adecuadas para la realización de las transferencias internacionales.

SANCIONES DE LA AEPD

# 9.000 euros por publicar imágenes en una web sin el consentimiento de la afectada

En el procedimiento sancionador https://www.aepd.es/es/documento/ps-00279-2020.pdf se sanciona con una cuantiosa cantidad al propietario de una URL por incumplir la normativa de protección de datos.

**La reclamante solicitó al propietario de la web que suprimiera todos sus datos personales, lo que incluía también material fotográfico, puesto que, no contaba con su consentimiento. Una vez ejercido su derecho de supresión no obtuvo respuesta alguna, por lo que inicia la reclamación ante la AEPD**. Además, en el escrito de su reclamación indica que la página web no cumplía con los requisitos de información que debe facilitar el responsable cuando recoge datos de carácter personal.

La AEPD notifica el acuerdo de inicio del procedimiento al reclamado, durante el plazo indicado no recibe ningún tipo de alegaciones por su parte, con lo cual, se convierte en propuesta de resolución.

La cantidad impuesta asciende a un total de 9.000 euros por infracción muy grave de los siguientes artículos del RGPD:

- **5.000 euros por el incumplimiento del artículo 13 RGPD**; el responsable de la página web no cumple con el deber de información en su política de privacidad.
- **4.000 euros por el incumplimiento del artículo 6 RGPD**; el responsable de la página web publica imágenes sin haber obtenido previamente el consentimiento del interesado.

Son infracciones muy graves la omisión del deber de informar y la ilicitud del tratamiento de los datos personales.

**IMPORTANTE**

Los agravantes que se han tenido en cuenta en esta resolución han sido la acción negligente no intencional y los datos personales afectados (básicos-imagen).

LA AEPD ACLARA

# Consejos básicos para realizar reuniones online con privacidad y seguridad

En esta sección del boletín haremos referencia a las consultas que la AEPD ha ido resolviendo a través de la publicación de sus guías, así como otros artículos de interés editados por la AEPD en su página web.

En este caso, en la sección de innovación y tecnología, encontramos un documento de especial importancia para estos momentos, donde las reuniones virtuales online se han convertido en una constante habitual en las empresas. **Estas pueden suponer un grave riesgo para la confidencialidad de los asistentes si no se tienen en cuenta precauciones básicas para su preparación.** Estas reuniones pueden ser saboteadas, por antiguos compañeros de trabajo, o ciberdelincuentes.

En este documento se incluye una lista no exhaustiva para crear un espacio de trabajo eficaz y seguro.

- Seguir las políticas establecidas por la empresa utilizando solamente el proveedor tecnológico aprobado.
- Limitar la reutilización de los códigos/enlaces de acceso.
- Utilizar una "sala de espera" para ir admitiendo a los participantes y habilitar una notificación para cuando se unan a la reunión.
- Bloquear el acceso una vez que están todos los asistentes.
- No grabar la reunión, en tal caso informar a los asistentes de la finalidad.

**IMPORTANTE**

Durante la reunión desactive el micrófono y la cámara cuando no sea necesaria, en particular, si se realiza alguna acción fuera del foco de la cámara.

ACTUALIDAD LOPD

# La AEPD renueva sus videotutoriales para ayudar a configurar la privacidad en las app y redes sociales más utilizadas

*Fuente: AEPD*

**(Madrid, 2 de marzo de 2021)**. La Agencia Española de Protección de Datos (AEPD) ha renovado su catálogo de vídeos en los que ayuda a configurar las opciones de privacidad y seguridad de los principales sistemas operativos, navegadores web, redes sociales y aplicaciones más utilizadas.

Las nuevas tecnologías constituyen un elemento imprescindible en la vida diaria de millones de personas. El 64,7% de la población de 16 a 74 años utiliza redes sociales como Instagram, Facebook, Twitter o YouTube, según datos de 2020 de la 'Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares' del INE. Sin embargo, no todas las personas son conscientes de las opciones de privacidad que se ofrecen por defecto y qué pasos deben seguir si desean cambiarlas.

La Agencia, que ya contaba con una sección de videotutoriales para ayudar a los usuarios de estos servicios a modificar las opciones de privacidad, ha actualizado su repertorio de vídeos de los sistemas operativos Android e iOS; el navegador web Firefox; las redes sociales Facebook, Instagram y Twitter y la aplicación de mensajería instantánea WhatsApp. Asimismo, ha incorporado nuevos vídeos, como los de los navegadores Chrome y Edge, la aplicación de mensajería instantánea Telegram y la red social Tik Tok.

Los vídeos se inician con una breve introducción explicando qué es y para qué se utiliza cada servicio. A continuación, realizan un detallado repaso que guía a los usuarios paso a paso a través de las opciones de configuración de privacidad y seguridad de cada uno de estos servicios, ofreciendo recomendaciones para optar por el mayor grado de privacidad posible.

Cambiar los ajustes para que sólo nuestros contactos puedan ver nuestra foto de perfil o inhabilitar la hora de nuestra última conexión en WhatsApp; administrar quién puede ver la actividad de nuestro perfil en Facebook y de qué manera pueden encontrarnos y ponerse en contacto con nosotros el resto de usuarios; o activar la opción 'cuenta privada' en Tik Tok para que sólo los usuarios que aprobemos puedan seguirnos y ver los vídeos que publicamos son algunas de las opciones que se abordan en los vídeos.

Puede ver más información en el siguiente enlace

catálogo de vídeos para configurar las opciones de privacidad y seguridad

EL PROFESIONAL RESPONDE

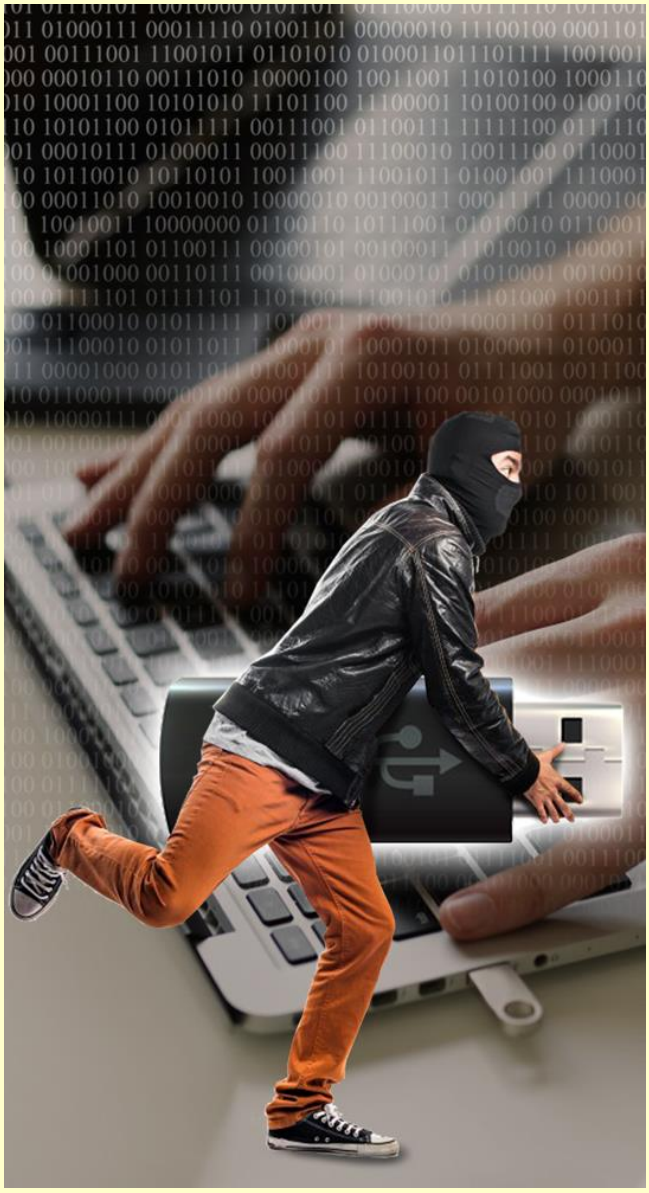
# Tipos de fuga de información y los escenarios posibles (I)

**Las fugas de información son uno de los incidentes de seguridad más comunes que suceden en las empresas. Estas se producen cuando se pierde la confidencialidad de la información de la empresa y esta es accesible a terceras personas no autorizadas.**

Estas fugas de información pueden ser involuntarias y no intencionadas, cuando, por ejemplo, se envía un correo a múltiples destinatarios sin copia oculta, o bien se pierde un dispositivo móvil o USB con información confidencial sin cifrar. Las fugas se consideran deliberadas cuando es un ciberdelincuente el que consigue acceder a los sistemas de la empresa, o bien, el conocido como insider, cuando se trata de un exempleado que pretende generar una pérdida de reputación.

**¿Cuáles son los escenarios principales donde se dan estas fugas? La información se puede extraer de las siguientes formas:**

- Dispositivos móviles y de almacenamiento externo.
- Correo electrónico
- Redes inalámbricas no confiables
- Aplicaciones en la nube o herramientas colaborativas
- Redes sociales
- Malware; troyanos, spyware, keyloggers
- Credenciales de acceso inseguras



**IMPORTANTE**

En el caso de ser víctima de una fuga de información o cualquier otra amenaza es recomendable interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado.