Boletín 02/22

LOPD EN LA EMPRESA

Altabir consulting

EL RGPD UE 2016/679 EN APLICACIÓN

Deber de secreto y seguridad en el ámbito laboral(I)

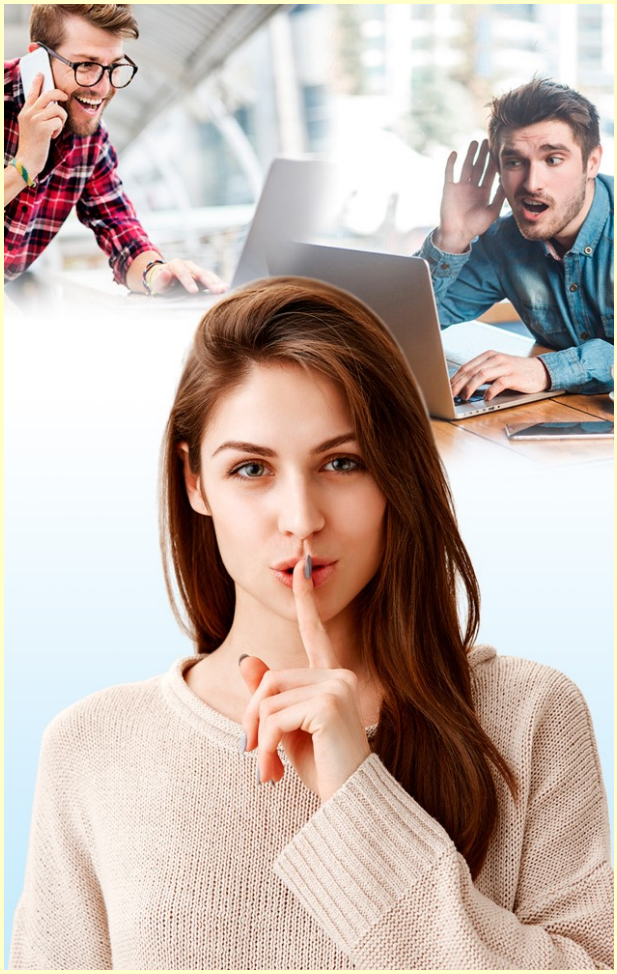
En nuestra LOPDGDD, el deber de secreto y confidencialidad está recogido en el artículo 5" Deber de confidencialidad". En él se detalla que los responsables y encargados del tratamiento y todas las personas que intervengan en cualquier fase del tratamiento están sujetas al deber de confidencialidad**. Es decir, todo el personal laboral de la empresa debe estar informado de este deber de confidencialidad. El responsable, además, en virtud de la proactividad tendrá que demostrarlo.**

La obligación general de confidencialidad será complementaria de los deberes de secreto profesional. Además, este articulo señala que las obligaciones de confidencialidad y de secreto profesional se mantendrán, aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

Por su parte, el responsable y encargado del tratamiento deben garantizar, no solamente, la confidencialidad, sino también, la disponibilidad de los datos, su pronta recuperación ante cualquier ataque y la integridad de los datos para que no puedan ser maliciosamente manipulados.

La empresa tiene que disponer de políticas de cumplimiento de estos dos principios.

Contenido



IMPORTANTE

La vulneración del deber de confidencial es considerada una infracción grave en la LOPDGDD.

SANCIONES DE LA AEPD

Sanción de 4.000€ a un taller mecánico por el envío de emails comerciales sin copia oculta

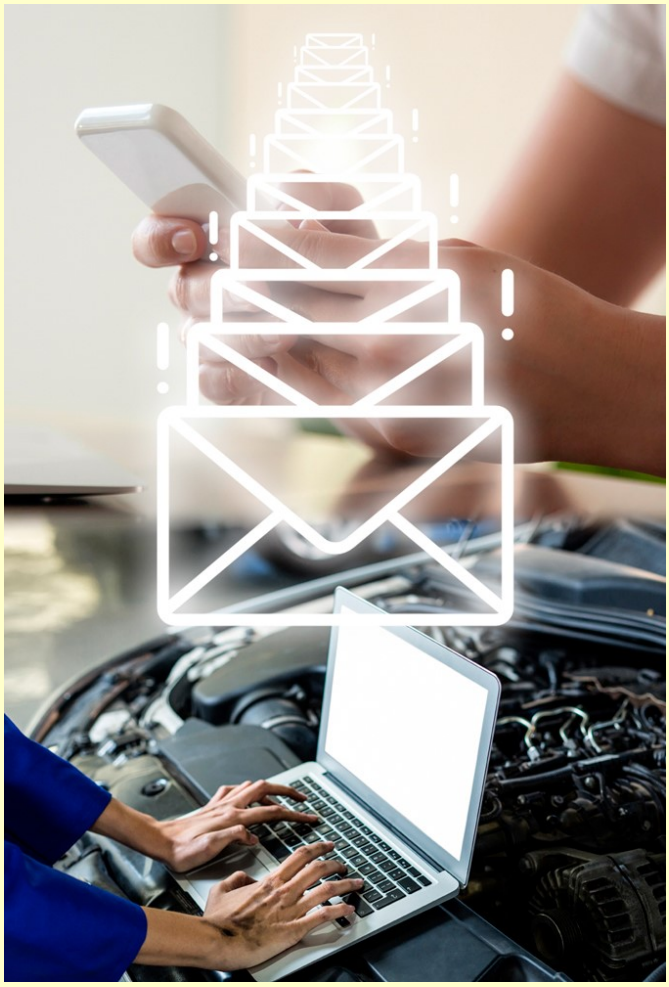
En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00259-2021.pdf, se sanciona a un taller mecánico por el envío de emails con carácter comercial, sin tener el consentimiento y, además, sin copia oculta.

El reclamante en su escrito de reclamación manifiesta que había recibido un correo comercial sin autorización previa. Además, estaban expuestos los datos de los demás destinatarios, incluyendo nombre y apellidos completos y dirección de correo electrónico. El reclamante en su escrito añadía, que no incluían ninguna opción para darse de baja. Como anexo a la reclamación, se adjuntan los datos completos del email recibido, con más de 400 destinatarios sin ocultar sus datos personales.

Se han incumplido varios preceptos del RGPD, por un lado, el principio de integridad y confidencialidad, unido a la falta de medidas de seguridad por parte del responsable para garantizar la confidencialidad de los datos personales. Como agravantes de la sanción se han tenido en cuenta el número de interesados afectados y la negligencia respecto a la gestión de la seguridad de los datos personales.

En este caso, además, el reclamante manifiesta que no dio su consentimiento para el envío de dichos correos comerciales, por lo que también la entidad es sancionada.

Principio de confidencialidad: tratar los datos que garanticen una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito.



IMPORTANTE

Para el envío de correos comerciales es necesario solicitar el consentimiento previo o bien existir una relación contractual previa.

LA AEPD ACLARA

Plan de Inspección de Oficio de la Atención Sociosanitaria (II) confidencialidad y obligaciones del personal

En el apartado de la AEPD Guías y Herramientas, encontramos el documento denominado "Plan de Inspección de Oficio de la Atención Sociosanitaria"

La confidencialidad en las operaciones de tratamiento en los centros sociosanitarios es un deber fundamental. **En estos centros se tiene un acceso generalizado a datos de categorías especiales. El cumplimiento del deber de confidencialidad debe llevarse al extremo.**

Aunque la mayoría de los colectivos profesionales que trabajan en los centros sociosanitarios están sujetos al secreto profesional, se debe complementar mediante un compromiso de confidencialidad escrito. **Este debe ser firmado por todos los empleados, becarios, estudiantes en prácticas, personal de empresas externas y en general, por cualquier persona con acceso a datos personales de los usuarios del centro. Los trabajadores sin acceso a datos personales, también deberían firmar un documento similar.**

Este documento debería contener:

-Prohibición general expresa de difundir, comunicar o revelar datos a terceras personas.

-Carácter indefinido del compromiso, inclusive extinguida la relación del trabajo con el centro.

-Información sobre las consecuencias y responsabilidades derivadas del incumplimiento.

IMPORTANTE

Se recomienda impartir formación e información sobre las obligaciones de protección de datos personales y entregar un acuse de recibo del documento informativo.

ACTUALIDAD LOPD

Cómo gestionar tus derechos ante la recepción de publicidad no deseada

Fuente: AEPD

A pesar de actuar de manera responsable a la hora de dar mis datos, no dar consentimiento para que los traten con finalidades publicitarias, inscribirme en la Lista Robinson y de haber seguido todos los consejos para prevenir la publicidad no deseada que presentábamos en esta entrega anterior de nuestro blog, es posible que sigas recibiendo algún tipo de comunicación comercial no deseada a través de llamadas de teléfono, mails, sms o mensajes a través de aplicaciones de mensajería instantánea.

A continuación, te presentamos una serie de consejos o acciones que puedes realizar para limitar la publicidad no deseada:

Utiliza las fórmulas que te ofrecen

Las comunicaciones electrónicas publicitarias ofrecen sistemas para que puedas rechazar el uso de tus datos con fines publicitarios, que incluyen medios como el envío de un correo electrónico a la dirección electrónica indicada, un SMS, un enlace o la opción de llamar a un número telefónico gratuito. Esta suele ser la manera más sencilla de dejar de recibir las comunicaciones comerciales de esa empresa, entidad u organización. Utilízala antes de pasar al resto de acciones que te presentamos.

Retira tu consentimiento

Si diste tu consentimiento cuando contrataste o te inscribiste en un servicio para que tratasen tus datos con fines publicitarios, puedes revocarlo en cualquier momento utilizando el método que la empresa ponga a tu disposición. Si desconoces o no encuentras la manera de hacerlo, puedes consultar el apartado dedicado a la protección de datos de su página web.

Ejerce tu derecho de oposición

Puedes ejercer este derecho ante la entidad responsable del tratamiento para solicitar que te excluya de las campañas publicitarias que realice. Si lo haces, indica claramente en la solicitud que no deseas que traten tus datos con fines publicitarios e informa del canal por el que estás recibiendo la publicidad y los datos que no deseas que se traten. Por ejemplo, si recibes publicidad telefónica, puedes indicar tu número de teléfono para que no lo utilicen con fines comerciales.

En el espacio dedicado a los derechos de nuestra web dispones de más información sobre el mismo y formularios tipo para ejercerlo ante el responsable. (…)

Puede ver más información en el siguiente enlace

Publicidad no deseada

EL PROFESIONAL RESPONDE

Los pilares de la Seguridad de la Información: confidencialidad, disponibilidad e integridad

Cuando escuchamos el término de Seguridad de la Información, casi de forma inmediata, se nos viene a la cabeza el término de confidencialidad de la información. Este es uno de los pilares en los que se sustenta la Seguridad de la información, pero no el único. La disponibilidad de la información y la integridad son dos aspectos de la información que también deben mantenerse a salvo.

La confidencialidad se refiere a que la información solo sea accesible al personal, entidades o sistemas autorizados para su acceso. Como ejemplo de esta falta de confidencialidad sería la divulgación no autorizada a través de las redes sociales de información confidencial, o el acceso por parte de un empleado a la información crítica de la empresa sin permiso asignado.

La disponibilidad de la información se refiere a que esta siempre esté accesible cuando la vayamos a utilizar. Como ejemplo de esta falta de disponibilidad, cuando existe un ataque de denegación de servicio y no podemos acceder a la información.

Y, por último, la integridad de la información supone que la información sea correcta y no sufra modificaciones no controlados o errores. Como ejemplo, podría ser la alteración de forma fraudulenta de los ficheros del sistema informático mediante la explotación de una vulnerabilidad.

IMPORTANTE

Se deben evaluar estas tres dimensiones de la información en los activos de información que emplea la empresa para implantar las medidas adecuadas.