PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 08/19

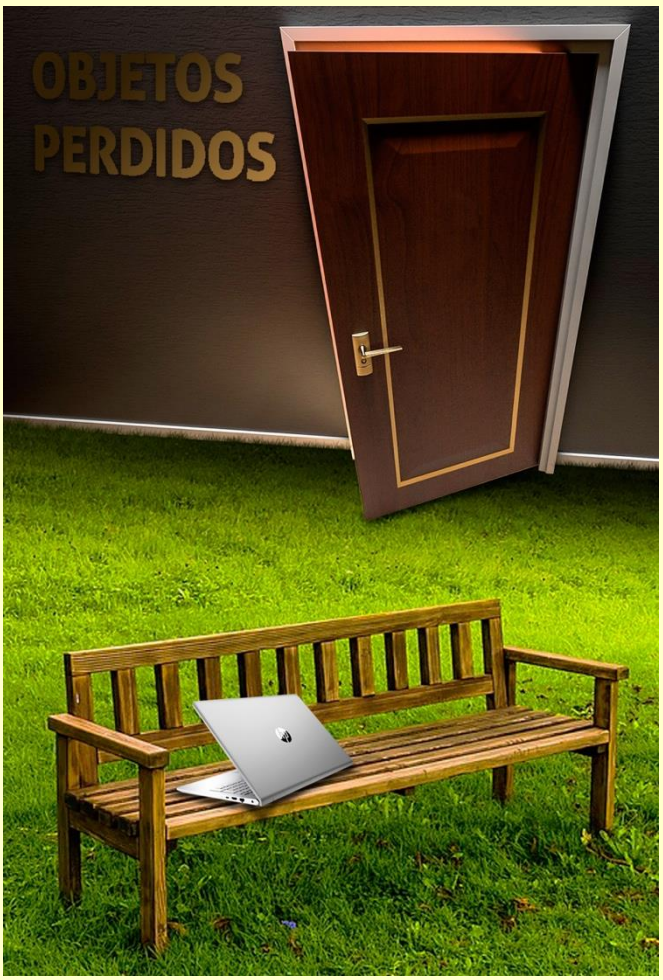
EL RGPD UE 2016/679 EN APLICACIÓN

¿Qué son Las brechas de seguridad? (I)

El término de brecha de seguridad se define en el art.4.12 del RGPD, como todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales, la conservación o tratamiento de forma ilícita, así como la comunicación o el acceso no autorizado a los datos, para que sea tenida en cuenta como brecha de seguridad, debe afectar a datos de carácter personal.

¿Qué han de tener en cuenta el responsable y encargado del tratamiento ante una brecha de seguridad? Independientemente del tamaño de la entidad y de la gravedad y consecuencias del incidente, el responsable y encargado del tratamiento lo tienen que dejar documentado en el registro de incidencias, incluyendo entre otros datos, los hechos relacionados con el incidente, sus efectos y las medidas correctivas que se han adoptado. Así, por ejemplo, la pérdida de un ordenador portátil, el acceso de un empleado no autorizado a la base de datos y su borrado, el envío de un e_mail a un destinatario incorrecto, constituyen todas brechas de seguridad que deben documentarse. Este documento lo pondremos a disposición de la autoridad de control, cuando ésta nos lo requiera, y verificar así, que cumplimos con lo dispuesto en la norma.

Contenido



IMPORTANTE

El encargado del tratamiento debe notificar las quiebras de seguridad al responsable, en caso de no comunicárselas se considera una infracción grave.

SANCIONES DE LA AEPD

GESTION DE COBROS, S.L. sancionada con 60.000 euros de multa por infringir la confidencialidad de los datos

La AEPD sanciona a la entidad GESTION DE COBROS,https://www.aepd.es/resoluciones/PS-00121-2019_ORI.pdf

La reclamante Dª.A.A.A., solicitó un mini préstamo por Internet a una empresa denominada "MARIA DINERO.COM", facilitándole sus datos personales, entre los cuáles se incluía su correo electrónico personal, pero no el de la entidad para la cuál trabaja, "La Universidad autónoma de Barcelona". En este último correo es donde la entidad sancionada, GESTION DE COBROS, le envía una notificación con la finalidad de reclamar la deuda con el asunto de Morosa. **El correo electrónico utilizado tiene carácter corporativo, por lo que todo el personal de la Universidad tiene acceso a su contenido, con lo cuál se ha cometido una infracción muy grave de confidencialidad de los datos de la reclamante.**

La AEPD al tener constancia de la reclamación, inicia un periodo de investigación, a partir del cual solicita información de los hechos a la entidad MARIA DINERO, ésta actúa correctamente, ya que informó a su cliente con carácter previo, que si no devolvía en plazo la cantidad prestada, sus datos serían comunicados a GESTION DE COBROS para recuperarlo, siendo ésta entidad la que no actúa diligentemente, puesto que, al utilizar el email del lugar de trabajo de Dª.A.A.A infringe el art.5.f del RGPD, ya que permitir a terceros, el acceso a los datos personales de la reclamante, causándole daños y perjuicios morales.

La sanción finalmente impuesta ha ascendido ha la cantidad de 60.000 euros, por los agravantes añadidos de nula cooperación con la autoridad de control y la intencionalidad de la infracción.

IMPORTANTE

La sanción ha sido calificada de muy grave al infringir, el principio de Confidencialidad de los datos, uno de los principales Principios recogidos en el RGPD.

LA AEPD ACLARA

¿Se pueden enviar comunicaciones comerciales electrónicas a los clientes sin su consentimiento?

La AEPD da respuesta en este informe https://www.aepd.es/media/informes/2018-0173-comunicaciones-comerciales.pdf a la consulta planteada por una entidad, en relación con el tratamiento de los datos de sus clientes con fines de mercadotecnia, publicidad y comunicaciones comerciales.

Lo primero que encontramos en este informe es la diferencia entre las comunicaciones comerciales realizadas por vía electrónica de aquellas, que tienen lugar por otros medios, ya que la legitimación y la ley principal que se aplica será diferente.

Las comunicaciones realizadas por vía electrónica, deben regularse por lo dispuesto en el art.21 de la LSSI, con lo que se convierte en ley especial sobre la norma general del RGPD. En este caso, el envío de comunicaciones comerciales solo podrá efectuarse con el consentimiento expreso del interesado o bien, cuando haya existido una relación contractual previa y los datos se hayan obtenido de forma lícita. Las comunicaciones tienen que referirse a productos o servicios de la propia empresa y que sean similares a los que fueron adquiridos con anterioridad.

Por otro lado, las comunicaciones comerciales realizadas por otros medios no electrónicos aplicarán el contenido del RGPD para el tratamiento de datos personales, así será el consentimiento expreso del interesado o bien el interés legítimo de la entidad, cuando no prevalezcan los intereses legítimos del interesado y exista una relación contractual previa.

IMPORTANTE

Debe garantizarse en todo momento al destinatario de los envíos comerciales, un procedimiento sencillo y gratuito para ejercer su derecho de oposición al tratamiento con fines de mercadotecnia directa.

ACTUALIDAD LOPD

Protección de datos en vacaciones

Fuente: https://www.aepd.es/blog/2019-07-24.html

Con la llegada de las vacaciones de verano cambiamos muchas de nuestras rutinas, viajamos, salimos más, visitamos lugares nuevos y disfrutamos de nuestro tiempo libre junto a familiares y amigos. En esta entrega de nuestro blog os presentamos algunos consejos sobre cómo afrontar situaciones de riesgo para la protección de nuestros datos personales en época estival.

Piensa dos veces antes de compartir una foto o vídeo

La actividad estival hace que la cámara de nuestro teléfono móvil tenga más trabajo del habitual: detalles de los lugares que hemos visitado, gente con la que hemos estado, fiestas a las que hemos asistido, etc. Compartir parte de esas fotografías (o todas) en una red social es algo habitual para algunas personas y entraña algunos riesgos.

Según datos del e Investigaciones Sociológicas (CIS), una de cada cuatro personas (24.5%) se ha arrepentido alguna vez de haber colgado algo en una red social. Te recomendamos que pienses en quién podrá ver tus fotos antes de pulsar el botón de compartir en tus redes sociales. Si tu perfil es accesible para los buscadores, ten en cuenta que cualquiera podrá ver, por ejemplo, las fotos, vídeos o comentarios que publicas. La Agencia dispone de una serie de vídeo tutoriales explicativos elaborados junto a INCIBE en los que explica cómo accceder a la configuración de privacidad y seguridad de algunos de los servicios más populares en Internet para que tu perfil no se muestre cuando, por ejemplo, introduzcan tu nombre en un buscador.

Una vez que tu perfil ya no sea accesible para los buscadores, piensa también en que las personas a las que das acceso a tu información eligen a su vez quien puede tener acceso a su perfil: amigos, amigos de amigos o todo el mundo. Si compartes una foto con tus seguidores o amigos en una red social y uno de ellos indica que algo le gusta, un amigo de amigo, al que no tienes por qué conocer, puede terminar viendo esa imagen. Y es posible que haya situaciones que quizás no quieres compartir con desconocidos.

Siguiendo con los datos del CIS, un 12.2% de los encuestados afirma haber tenido problemas por contenidos que otros han colgado en una red social. Debemos recordar que necesitamos consentimiento de las personas que aparecen en las fotos que tomamos antes de compartirlas en Internet o de sus padres o tutores en el caso en que aparezcan menores.

Puede ver más información en el siguiente enlace:

Protección de datos en vacaciones

https://www.aepd.es/media/infografias/Infografia-verano-AEPD.pdf

EL PROFESIONAL RESPONDE

¿Cuál es el significado en materia de protección de datos de observación habitual y sistemática?

Uno de los criterios que el RGPD utiliza para determinar si obligatoria, por ejemplo, la designación de Delegado de Protección de datos, o bien, la realización de una Evaluación de impacto, es cuando el tratamiento consista en una observación habitual y sistemática de interesados a gran escala o la observación sistemática a gran escala de zonas de acceso público.

En el RGPD no se define claramente el significado de habitual y sistemático, aunque si que encontramos alguna mención en sus considerandos cuando habla de observación del comportamiento de los interesados, como una forma de seguimiento y creación de perfiles en internet, pero no solamente tenemos que quedarnos en ese ámbito.

El Grupo de trabajo del art.29, el actual Comité Europeo, nos da unas pistas de lo que pueden significar dichos términos:

Habitual: continuado o que se produce a intervalos concretos durante un periodo concreto; recurrente o repetido en momentos prefijados.

Sistemática: que se produce de acuerdo a un sistema; preestablecido, organizado o metódico.

Algunas actividades que constituyen una observación habitual y sistemática, serían, por ejemplo, las aplicaciones móviles que realizan un seguimiento de la ubicación del usuario y los dispositivos ponibles que analizan nuestros datos de bienestar, estado físico y salud.

IMPORTANTE

Los desarrolladores de aplicaciones que realicen este tipo de actividades de seguimiento, tendrán que cumplir con todos los requisitos que exige la normativa en materia de protección de datos.