Boletín 10/18

LOPD EN LA EMPRESA

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

Altabir consulting

www.altabir.es

EL RGPD UE 2016/679 EN APLICACIÓN

Regulación de transferencias de datos a terceros países (III)

En el caso de que **no existan decisiones de adecuación o garantías adecuadas**, el **RGPD regula unas excepciones para situaciones específicas,** que nos permitirán realizar una transferencia de datos personales a un tercer país u organización internacional.

Excepciones previstas en el art.49 RGPD

1ºCon el consentimiento del interesado, una vez que ha sido informado de los posibles riesgos.

2º Necesitamos hacer la **transferencia para la ejecución de un contrato entre el interesado y el responsable**.

3º Es necesaria para la **ejecución de un contrato entre el responsable y otra persona física o jurídica, en interés del interesado.**

4º Cuando existan **razones importantes de interés público.**

5ºEs requerida para **la formulación, ejercicio o defensa de reclamaciones**.

6º Se precisa para **proteger intereses vitales del interesado,** cuando esté física o jurídicamente incapacitado.

7º Cuando se **realice desde un registro público** y esté abierto a la consulta del público en general, atendiendo al Derecho de la Unión o Estados miembros.

Contenido

IMPORTANTE

Además de ofrecer garantías apropiadas en protección de datos, tendremos que **informar a la autoridad de control, cuando no se pueda aplicar ninguna de las excepciones**

SANCIONES DE LA AEPD

La Audiencia Nacional ratifica los 30.000 euros de multa impuestas por la AEPD a dos empresas de telemarketing

Recientemente hemos conocido **el fallo de la sala primera de lo contencioso administrativo de la Audiencia Nacional, que ratifica las multas que la AEPD** impuso en su procedimiento sancionador **contra dos empresas de telemarketing: Crosseling Operadores 3.9 SLU y Global Telemarketing Solutions,** subcontratada por la primera.

La sentencia absuelve a Orange, ya que no autorizó la subcontratación que Crosseling realizó con Global Telemarketing para la acción comercial multada.

En ese procedimiento **la AEPD declaraba que ambas entidades habían infringido el** ***art.48.1b de la LGT***, al no tener en cuenta, **la inscripción del demandante en la Lista Robinson Aidigital** así como, su derecho de oposición, puesto que **habían seguido realizando llamadas de carácter comercial a su teléfono fijo en nombre de Orange.** Además, tampoco cumplieron con lo dispuesto en el ***art.49.4 RDLOPD*****, que obliga a aquellos que pretendan hacer una prospección comercial a consultar previamente los ficheros comunes** que afecten a esa actuación, por ejemplo, la mencionada Lista Robinson Aidigital.

Las dos empresas **rechazaban el argumento de la intencionalidad, gravedad así como del beneficio para la empresa y daño para el usuario en su actuación,** sin embargo, la **AEPD, sí que entiende que existía esa intencionalidad**, ya que como profesionales del sector del marketing telefónico **deberían conocer y cumplir las normas vigentes que regulan su actividad**, tales como la LGT y la LOPD, además del **daño ocasionado al demandante al realizar llamadas en horarios que se interponían con su vida diaria, puesto que trabajaba a turnos, impidiéndole el descanso.**

IMPORTANTE

Siempre que se vayan a realizar **campañas de carácter comercial**, tenemos que **asesorarnos y ser conscientes de la base de datos personales a utilizar** y comprobar por todos los medios, que cuenta con los permisos legales oportunos.

LA AEPD ACLARA

Publicación en la página del Ministerio de educación de beneficiarios de becas destinadas a los alumnos/as con necesidades especiales

El informe 2017-240 resuelve acerca de si es posible **publicar en la página web del Ministerio de Educación, Cultura y Deporte, los datos personales,** incluidos los **datos de salud**, de las personas a las que se les había concedido las ayudas de apoyo educativo para el **curso académico 2017-2018, reguladas por la resolución de la convocatoria del 3 de agosto de 2017.**

En este sentido, **la AEPD viene a analizar en su informe que se entiende por publicación,** según la ***Ley 39/2015, 1 octubre del procedimiento administrativo común de las administraciones públicas***, la publicación será **obligatoria cuando nos encontremos ante actos integrantes de un procedimiento selectivo** o de concurrencia competitiva, tal y como serían, por ejemplo, las subvenciones, sin embargo **el caso de la consulta, según el régimen de concesión de becas y ayudas al estudio, siempre y cuando no se fije un número determinado de beneficiarios, se concederán de forma directa,** por lo que **no existe, esa concurrencia competitiva.** Por lo que la **notificación** a los interesados por parte del ministerio, **deberá procederse a realizar de forma individual.**

Así mismo, para cumplir con la **Ley de Transparencia**, **la publicidad activa** que se haga de estas concesiones cuando haya **datos de salud, se realizará siempre de forma disociada.**

IMPORTANTE

Todas las **Administraciones públicas estatales, autonómicas y locales,** deben de cumplir con lo dispuesto en la **normativa de protección de datos personales, en lo que se refiere a su publicación**

ACTUALIDAD LOPD

Medidas de seguridad en Facebook

Fuente: AEPD

Desde la Agencia te recomendamos que cierres las sesiones abiertas en todos tus dispositivos y vuelvas a introducir las credenciales si quieres volver a acceder

---

El pasado viernes Facebook hizo pública una brecha de seguridad en su red social que podría haber dejado al descubierto información de 50 millones de usuarios. Según la información hecha pública por la compañía, los atacantes explotaron una vulnerabilidad en el código de Facebook para robar 'tokens' de acceso a Facebook, a través de los que podían acceder a las cuentas de las personas.

Facebook ha anunciado que ha reiniciado los tokens de acceso de casi 50 millones de cuentas y restablecido los de otros 40 millones como medida de precaución. Los tokens de acceso son una herramienta que permiten no tener que identificarse cada vez que se accede a la red social desde el dispositivo, manteniendo las sesiones abiertas.

Es importante dejar claro que son aquellos que tratan los datos de los ciudadanos los encargados de velar por la privacidad y seguridad de los mismos. El ciudadano, por su parte, también puede tener un papel activo en su protección, por lo que no está de más recordar una serie de precauciones adicionales. Desde la Agencia recomendamos, en primer lugar y como medida básica en este caso de Facebook, **cerrar la sesión que se tenía abierta en la red social y volver a introducir las credenciales si se desea volver a acceder**.

La Oficina de Seguridad del Internauta (OSI) ha publicado una serie de consejos en caso de que el usuario tenga problemas para iniciar su sesión o que quiera revisar en qué dispositivos se ha iniciado sesión con nuestra cuenta. Por otro lado, y aunque se ha difundido que no es necesario cambiar la contraseña de acceso a la red social, aprovechamos para recordar las fichas 2 y 3 de la Guía de privacidad y seguridad en Internet, elaborada por la Agencia e INCIBE, en las que se recogen consejos sobre la creación de contraseñas robustas. Además, en este vídeo te explicamos cómo puedes configurar tu privacidad en Facebook y, si quieres saber cómo revisar la configuración de tu perfil para gestionar la información que Facebook sabe de ti, puedes seguir estos consejos.

Puede ver más artículos relacionados en los siguientes enlaces:

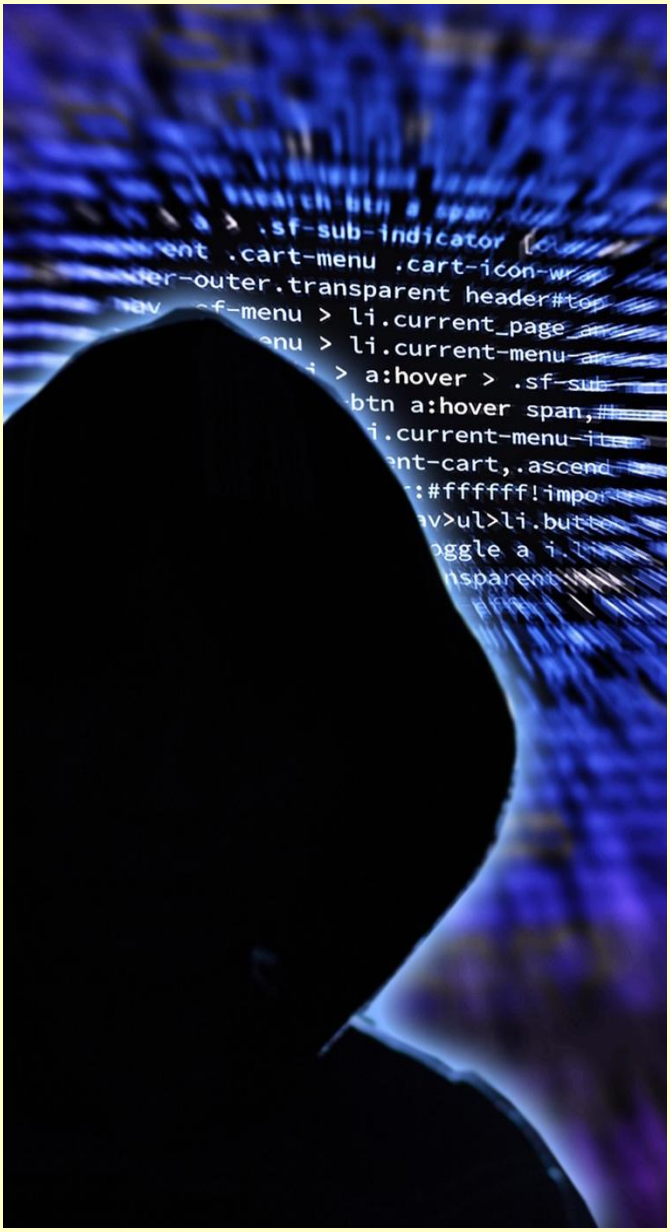
Video Configurar la privacidad en Facebook

Guía de la Privacidad y Seguridad en Internet

EL PROFESIONAL RESPONDE

Qué son las brechas de seguridad, detección y clasificación

Lo primero que tenemos que conocer es el significado de lo que es una brecha de seguridad, en el RGPD encontramos la siguiente definición en su art.4.12 “toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos”.



La guía de la AEPD nos orienta para realizar su detección, bien a través de las fuentes internas de la empresa, tales como un consumo excesivo de memoria o disco en servidores, alertas generadas por software antivirus, entre otras. También se detectan a través de las fuentes externas, por ejemplo, comunicación de un incidente por parte del encargado de tratamiento que nos presta un servicio informático.

La clasificación de las brechas de seguridad podría ser:

- Brecha de confidencialidad: cuando las partes no autorizadas o sin un propósito legítimo acceden a la información. La gravedad dependerá del número potencial y el tipo de partes que hayan accedido a la misma.
- Brecha de integridad: se altera la información original, pudiendo ocasionar un daño al interesado.
- Brecha de disponibilidad: no se puede acceder a los datos originales cuando se necesita.

IMPORTANTE

Notificaremos las brechas de seguridad en un plazo de 72hrs. a la AEPD, siempre y cuando suponga un riesgo para los derechos y libertades de las personas físicas.