Boletín 11/17

LOPD EN LA EMPRESA

Balaguer & Gutiérrez
Correduría de Seguros
Consultoría de Protección de Datos

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

LA LOPD EN EL DÍA A DÍA

Tratamiento de datos de menores en el nuevo RGPD

Una de las novedades importantes en el nuevo Reglamento Europeo de Protección de Datos es la **obligación de obtener el consentimiento expreso** al recabar datos personales, siendo necesaria una **clara acción o declaración afirmativa, ya sea** mediante el marcado de una casilla en un sitio web, una firma documental, etc.

El artículo 8 del Reglamento establece las **condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información** y dispone que:

1. Será **lícito el tratamiento de datos personales de un niño mayor de 16 años**. Si el niño fuera menor, será necesario el consentimiento del titular de la patria potestad o tutela para tratar sus datos.

2. **Los Estados miembros podrán establecer una edad inferior**, siempre que ésta **no esté por debajo de los 13 años**.

3. El responsable del tratamiento **deberá esforzarse para verificar que el consentimiento fue dado o autorizado** por sus padres o tutores legales.

4. La edad para tratar datos de un menor es independiente de las **normas relativas al Derecho contractual o laboral** de los Estados miembros (como son las normas relativas a la validez o efectos de los contratos en relación con un niño).

Contenido

IMPORTANTE

Hoy día en España, el Real Decreto 1720/2007, mantiene la edad de 14 años para poder tratar datos directamente del menor sin autorización de sus padres o tutores

SANCIONES DE LA AEPD

Sanción por cesión de datos a empresa de publicidad comercial a través de internet

En el PS/00302/2017 de la AEPD, vemos la sanción impuesta a la entidad ENLARED AUTO 10 S.L., dedicada a la venta de automóviles on line por **ceder datos de sus clientes a la entidad LEAD CONVERSION, S.L. (LEAD S.L.) para el envío de correos electrónicos de sus campañas publicitarias sin consentimiento de los titulares**.

Obtener el consentimiento de los titulares es esencial antes ceder datos personales a otra entidad para su propio uso

En octubre de 2016 entra en la Agencia escrito de un afectado que denuncia haber recibido 17 correos electrónicos con información comercial sobre productos y servicios de telefonía, seguros de salud, viajes y alojamientos, muebles remitidos desde una cuenta perteneciente a la entidad LEAD S.L. que no han sido solicitados o autorizados previamente por él.

La AEPD inicia la investigación **requiriendo a LEAD S.A. que le informe sobre el origen de la dirección de correo del denunciante y el consentimiento para el envío** de comunicaciones comerciales.

LEAD aporta copia del contrato con ENLA REDAUTO 10, S.L. en el que se establece la prestación de servicios de intermediación comercial autorizándole **a LEAD S.L. para que designe los destinatarios finales de todas sus campañas.**

El denunciado, responsable del tratamiento de los datos del denunciante **ha realizado una comunicación de datos de direcciones de correos electrónicos a LEAD, S.L. para su propio uso y beneficio sin poder acreditar el consentimiento** de los interesados.

RESULTADO: multa de 3.000 € a ENLARED AUTO 10, S.L., por una infracción del artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3.b) de la LOPD de conformidad con lo establecido en el artículo 45 apartados 2 y 5 de la citada LOPD.

IMPORTANTE

Es obligación del responsable del tratamiento poder demostrar que recabó el consentimiento de los interesados antes de comunicar los datos a un tercero

LA AEPD ACLARA

Ley de Transparencia y Protección de Datos

El Informe Jurídico 0178/2014 de la AEPD plantea varias cuestiones relativas a **cómo afecta la Ley 15/1999 a la aplicación de la Ley 19/2013, de transparencia,** acceso a la información pública y buen gobierno.

La Ley 19/2013 **regula el derecho de acceso a la información pública por parte de todos los ciudadanos,** la cual será publicada en las correspondientes sedes electrónicas o páginas web de las distintas Administraciones Públicas.

En dicha información se **encontrarán publicados datos de carácter personal de los obligados y otras personas físicas.**

¿Cómo afecta esto a la protección de Datos?

-Los datos de personas que se hagan públicos, **estarán sometidos a la LOPD.**

-Su publicación o cesión en la web **está legitimada en el art. 11.2 a) de la LOPD**, pues la publicación de información está prevista en la Ley de Transparencia 19/2013, que no sólo la autoriza, sino que establece los criterios que regirán dicha publicidad.

-Si esa información **contiene datos de salud (de beneficiarios de subvenciones,** por ejemplo), **deberá procederse a su disociación**, a menos que se cuente con el consentimiento previo.

-**Podrá ejercitarse el derecho de acceso a los datos**, pero teniendo en cuenta otras leyes referidas al derecho de información.

-La normativa de protección de datos será de aplicación al tratamiento posterior de los datos obtenidos a través de dicho derecho de acceso

IMPORTANTE

Los datos de carácter personal objeto del tratamiento, podrán ser tratados sin el consentimiento de su titular cuando la cesión esté autorizada o prevista en una ley.

ACTUALIDAD LOPD

La AEPD sanciona a Google por tratar sin consentimiento datos personales recogidos a través de redes WiFi con los coches de su servicio Street View

Fuente: *www.agpd.es*

La AEPD sanciona a Google por tratar sin consentimiento datos personales recogidos a través de redes WiFi con los coches de su servicio Street View

La Agencia constata que Google almacenó datos personales transmitidos a través de redes WiFi abiertas sin que los afectados tuviesen conocimiento de dicha recogida.

- La Agencia ha constatado que Google captó y almacenó sin consentimiento datos personales de los ciudadanos procedentes de redes inalámbricas a través de los vehículos empleados en su proyecto Street View
- El procedimiento declara la existencia de una infracción grave de la Ley de Protección de Datos e impone a Google una sanción de 300.000 euros
- La AEPD se vio obligada a dejar en suspensión la tramitación de este procedimiento administrativo en 2010 tras la presentación de una denuncia por la vía judicial penal, resolviéndolo una vez adoptada la resolución judicial

(Madrid, 7 de noviembre de 2017). La Agencia Española de Protección de Datos (AEPD) ha dictado una resolución que pone fin al procedimiento abierto a la empresa Google en relación a la recogida y tratamiento de datos personales de redes WiFi llevada a cabo por los vehículos empleados en el proyecto Street View. En el marco de la investigación realizada, la AEPD ha constatado que Google recogió y almacenó datos personales transmitidos a través de redes WiFi abiertas sin que los afectados tuviesen conocimiento de dicha recogida y sin obtener el consentimiento de los mismos. En consecuencia, la Agencia **declara la existencia de una infracción grave** e impone a Google una sanción de 300.000 euros.

La AEPD inició de oficio la investigación de estos hechos en mayo de 2010. No obstante, la existencia de un procedimiento judicial penal abierto en el Juzgado de Instrucción Nº 45 de Madrid obligó a la AEPD a suspender la tramitación de su procedimiento sancionador en virtud del artículo 7 del Real Decreto 1398/1993, por el que se aprueba el Reglamento del Procedimiento para el Ejercicio de la Potestad Sancionadora. Una vez se tuvo conocimiento de la firmeza del auto por el que se acuerda el sobreseimiento provisional y archivo de las diligencias previas, la Agencia Española de Protección de Datos ha reanudado el procedimiento administrativo, resolviéndolo tras el correspondiente plazo de presentación de alegaciones.

La Ley Orgánica de Protección de Datos establece en su artículo 6.1 que el tratamiento de los datos de carácter personal **requiere el consentimiento inequívoco del afectado**, salvo determinadas excepciones no aplicables en este caso concreto. En el marco de la investigación realizada, la Agencia Española de Protección de Datos ha constatado que **Google recogió información de diversa tipología** sin que los afectados tuviesen conocimiento de que dicha recogida de datos se estaba llevando a cabo y sin su consentimiento. La compañía recabó, entre otra, información relativa a direcciones de correo electrónico de personas físicas, códigos de usuario y contraseña que permiten el acceso a cuentas de correo electrónico, direcciones IP, direcciones MAC de los routers y de los dispositivos conectados a los mismos o nombres de redes inalámbricas (SSID) configurados con el nombre y apellidos de su responsable. No se ha constatado que Google tratase datos especialmente protegidos a través de estos sistemas.

Puede ver más información en el siguiente enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_11_07-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Qué es una Evaluación de Riesgos?

Como consecuencia del desarrollo de la tecnología, **los datos de carácter personal adquieren cada día un mayor valor económico para las empresas,** siendo necesaria la **adopción de nuevas medidas que contribuyan a su protección** y por tanto, al respeto de los derechos de las personas.

Para ello son útiles algunas herramientas nacidas a raíz de la nueva legislación europea sobre Protección de Datos como las **"Evaluaciones de Impacto en la Privacidad" (EIPD).**

Una EIPD consiste en:

1- La **realización de un análisis de los riesgos** que un determinado sistema de información, un producto o servicio que va a salir al mercado, puede suponer para el derecho fundamental a la protección de datos

2- **Tras ese análisis, se ha de llevar a cabo una gestión eficaz** de los riesgos que se hubieran identificado

3- Una vez identificados**, se deberán adoptar las medidas necesarias para eliminarlos o mitigarlos**

Una EIPD se requerirá en caso de que las empresas lleven a cabo tratamientos de:

- **Elaboración de perfiles** y análisis automatizado de aspectos personales de individuos
- **Categorías especiales de datos** personales a gran escala
- **Observación sistemática de zonas de acceso público** a gran escala

IMPORTANTE

El informe final de la EIPD debe ser remitido a la alta dirección de la empresa para que tome las decisiones necesarias sobre las medidas sugeridas por el equipo