Boletín 12/17

LOPD EN LA EMPRESA

Autor: Julio César Miguel Pérez

Balaguer & Gutiérrez
Correduría de Seguros
Consultoría de Protección de Datos

LA LOPD EN EL DÍA A DÍA

Cuándo es necesario nombrar un DPO en la empresa

Contenido

Una de las novedades importantes que introduce el nuevo RGPD (UE) 2016/679, de 27 de abril de 2106, cuya entrada en vigor está prevista para el 25 de mayo de 2018, es la designación o contratación de una **figura encargada de informar y asesorar a los Responsables y encargados del tratamiento acerca de las obligaciones para cumplir con dicho Reglamento**. Es la figura del DPO o Delegado de Protección de Datos

La cuestión que genera gran inquietud es si **todas las entidades necesitan nombrar a esta figura o sólo alguna en particular**.
El art. 37.1 del RGPD establece de forma expresa que el responsable y el encargado del tratamiento designarán un DPD siempre que:

a) **el tratamiento de datos sea realizado por una autoridad u organismo público**, excepto los tribunales cuando actúen en ejercicio de su función judicial

b) las actividades del responsable o del encargado consistan en **tratamientos de datos que requieran una observación habitual y sistemática de interesados a gran escala** (videovigilancia a gran escala)

c) las actividades del responsable o del encargado consistan en el **tratamiento a gran escala de categorías especiales de datos personales e infracciones penales**

IMPORTANTE
El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

SANCIONES DE LA AEPD

Sanción por recoger datos de menores sin consentimiento

En el **PS/00339/2011** de la AEPD vemos la sanción que sufre una entidad por **recoger datos de menores de edad sin obtener el consentimiento paterno previo.**

Las entidades responsables deberán establecer procedimientos para recoger datos personales y ejercer los derechos ARCO.

Con fecha 1 de febrero de 2011 se recibe en el registro de la Agencia Española de Protección de Datos escrito de reclamación de D. A.A.A., en el que pone de manifiesto que durante el mes de diciembre de 2010 y comienzos de enero de 2011, **el canal infantil de televisión TDT BOING** promocionaba la **asistencia a la Cabalgata de Reyes** en una carroza patrocinada por la cadena. **Para participar** en el concurso, **se debía cumplimentar un formulario disponible en la web www.boing.es**, el cual recogía datos personales de menores puesto que en las bases de la promoción figuraba que iba dirigido a niños entre 7 y 12 años. No obstante**, no se solicitaba el consentimiento del tutor legal ni se facilitaba claramente la finalidad de la recogida ni la información necesaria para ejercitar los derechos ARCO.**

En la inspección de la AEPD se comprueba que **aunque el sitio web www.boing.es es un portal dirigido a un público juvenil cuya información facilitada en la recogida de datos se realiza cumpliendo la LOPD**, sin embargo, **en la recogida de datos para participar**, en fechas del 15 de diciembre hasta el 26 de diciembre de 2010, en la promoción de la Cabalgata de Reyes en Madrid para menores entre 7 y 12 años, era necesario **rellenar un formulario con datos personales, no existiendo ninguna opción para solicitar la autorización** del padre/madre/tutor, **ni constaba la información establecida por la LOPD**.

Resultado: Sanción de 20.000 € por una infracción del artículo 6.1 de la LOPD

IMPORTANTE

Se ha de ser especialmente cauto a la hora de recoger y tratar datos personales y especialmente de menores de 14 años

LA AEPD ACLARA

Puede una empresa solicitar a un demandante de empleo certificado de antecedentes penales?

El Informe Jurídico 0401/2015 de la AEPD resuelve sobre **si puede una empresa solicitar el certificado de antecedentes penales o el certificado negativo del Registro Central de delincuentes sexuales** a aquellas personas que pretenden acceder a puestos de trabajo en ella, de conformidad con la LOPD.
Para aclarar esta cuestión es necesario valorar la actividad de la empresa y cada puesto de trabajo concreto. Existen dos posibilidades:

-Si se pretende acceder y ejercitar **profesiones, oficios o actividades que impliquen contacto habitual con menores**, el requerimiento de los datos en cuestión, **estaría legitimado por ley**, pues la LO1/1996, de Protección Jurídica del Menor, modificada en 2015, establece como requisito para acceder y ejercitar dichas profesiones, no **haber sido condenado por sentencia firme por algún delito contra la libertad e indemnidad sexual** y por tanto, quien pretenda el acceso a tales profesiones deberá acreditar esta circunstancia aportando una certificación negativa del Registro Central de delincuentes sexuales.

-Ahora bien, **en el caso de que no sea necesario el contacto habitual con menores para el desempeño de la actividad** o puesto solicitado, no resultará posible exigir dicho certificado, pues el tratamiento de estos datos no tiene habilitación legal, pudiendo ser tratados estos datos solamente por la Administración Pública.

IMPORTANTE

Los datos personales relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas

ACTUALIDAD LOPD

El Esquema Nacional de Seguridad recoge las medidas que debe aplicar el sector público para cumplir con los requisitos del RGPD en este ámbito

Fuente: *www.agpd.es*

El Esquema Nacional de Seguridad recoge las medidas que debe aplicar el sector público para cumplir con los requisitos del RGPD en este ámbito

El CCN-CERT y la AEPD establecen un mecanismo de colaboración para ofrecer a las Administraciones Públicas una referencia de cumplimiento normativo en materia de protección de datos y seguridad.

- La herramienta PILAR para Administraciones Públicas incluye desde hoy un módulo para facilitar el cumplimiento
- El Reglamento General de Protección de Datos (RGPD), que establece nuevos requisitos, será aplicable el 25 de mayo de 2018

(Madrid, 12 de diciembre de 2017). El CCN-CERT y la Agencia Española de Protección de Datos (AEPD) han establecido un mecanismo de colaboración con el objetivo de ofrecer a las Administraciones Públicas una referencia de cumplimiento normativo en materia de protección de datos y seguridad ante la próxima entrada en vigor del Reglamento General de Protección de Datos (RGPD) el 25 de mayo de 2018.

El Esquema Nacional de Seguridad y el RGPD establecen la obligación de que las Administraciones Públicas realicen análisis de riesgos para determinar el posible impacto de los tratamientos de datos sobre los derechos y libertades de las personas y las medidas de seguridad aplicables.

En este sentido, la AEPD ha publicado un documento en el que pone de manifiesto que esas medidas de seguridad –en el caso de las AAPP– estarán marcadas por los criterios establecidos en el Esquema Nacional de Seguridad. El Proyecto de Ley Orgánica de Protección de Datos, actualmente en fase de tramitación, lo recoge de la misma forma en su disposición adicional primera.

Fruto de la colaboración, el CCN-CERT y la AEPD han trabajado de forma conjunta para ofrecer una herramienta a las Administraciones Públicas que les permita evaluar de manera sistemática y objetiva los posibles riesgos en materia de protección de datos y de seguridad de la información. Así, la herramienta PILAR incluye desde hoy un módulo de cumplimiento que permite a las AAPP verificar los requisitos establecidos en el RGPD, facilitando la gestión normativa tanto del Reglamento como del Esquema Nacional de Seguridad.

La obligatoriedad de contar con un registro de actividades de tratamiento, designar un Delegado de Protección de Datos o notificar las quiebras de seguridad en caso de producirse son algunos de los aspectos recogidos en este nuevo módulo.

Puede ver más información en el siguiente enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_12_12-ides-idphp.php

EL PROFESIONAL RESPONDE

¿Pueden incluirme en un grupo de WhatsApp sin mi permiso?

La creación de un grupo de **WhatsApp por una entidad pública o privada, tiene relación directa con la protección de datos personales**, pues en el momento en el que alguien te agrega a dicho grupo, tanto tu número de teléfono, como tu foto de perfil, serán accesibles por el resto de personas que lo forman, algunas de las cuales, quizás ni siquiera conoces.

A efectos de la LOPD **esto es considerado una cesión de tus datos personales**, para lo que legalmente **es preciso el permiso o consentimiento del titular de los datos**.

La Agencia Española de Protección de Datos (AEPD) acaba de dictar una resolución en la que analiza esta situación y concluye con la **existencia de varias infracciones**:

- **Tratamiento de datos de carácter personal sin recabar consentimiento de** los afectados
- **Revelación de datos personales** infringiendo el deber de secreto al que está obligado el responsable
- **Tratamiento de datos para fines diferentes** para los que los mismos fueron recabados
- **Cesión de datos sin contar con el consentimiento del interesado**

Por ello, **antes de crear un grupo de WhatsApp**, salvo que tenga fines personales o domésticos, **deberá ser aceptado por todos sus componentes**.

IMPORTANTE

La creación de un grupo de WhatsApp tiene también un marco legal que respetar, al menos en materia de protección de datos personales