LOPD EN LA EMPRESA

EL RGPD UE 2016/679 EN APLICACIÓN

¿Por qué son importantes los contratos de acceso a datos? (I)

En caso de que el responsable del tratamiento necesite externalizar algunos de sus servicios o funciones y ello conlleve el tratamiento de datos personales será imprescindible que se formalice un contrato de acceso a datos por cuenta de terceros, también conocido, como contrato de encargado de tratamiento.

En el artículo 28.3 del RGPD se regulan todas las cláusulas que este contrato de acceso a datos ha de contener. Entre otros aspectos, se tiene que establecer:

- El objeto, la duración, la naturaleza y la finalidad del tratamiento.
- El tipo de datos personales y categorías de interesados.
- Las obligaciones del encargado de tratamiento.
- Las obligaciones del responsable del tratamiento.

Además, en particular, se indicará que el encargado del tratamiento ha de seguir únicamente las instrucciones indicadas por el responsable, incluso respecto a las transferencias de datos personales a un tercer país o una organización internacional.

En posteriores boletines desarrollaremos las obligaciones de cada uno de los roles del contrato.

Contenido

IMPORTANTE

Se considera una infracción grave encargar el tratamiento de datos de un tercero sin la previa formalización de un contrato de acceso a datos.

SANCIONES DE LA AEPD

Sancionado un encargado de tratamiento por no regular un contrato de acceso a datos con un subencargado

En la resolución de la AEPD https://www.aepd.es/es/documento/reposicion-ps-00668-2022.pdf, se sanciona a una empresa que gestionaba el servicio de asesoría, apoyo comercial y técnico para la captación de clientes incluida la realización de acciones de venta telefónica en nombre de una compañía suministradora de luz y gas.

La reclamación fue interpuesta por una potencial cliente de la suministradora de luz y gas a la que mediante una venta telefónica le ofrecieron un contrato, que finalmente canceló a los pocos días.

La venta final no fue realizada por la compañía suministradora de luz y gas ni por su encargada de tratamiento, sino por otra empresa tercera que actuaba de subencargada sin haber celebrado ningún contrato de acceso a datos y sin haberlo comunicado a la compañía en virtud de la cual se estaban tratando los datos.

En el contrato de acceso a datos que la compañía suministradora de luz y gas tenía regulado con su encargado de tratamiento se prohibía recurrir a la subcontratación, y en el caso de que fuera necesaria, se debería solicitar una autorización con una antelación mínima de un mes.

La AEPD desestima el recurso de reposición sancionando al encargado del tratamiento con una multa de 10.000€ por no haber comunicado la subcontratación a la compañía suministradora de luz y gas.

El encargado del tratamiento está obligado a informar sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.

IMPORTANTE

Se considera una infracción grave la contratación por un encargado de tratamiento de otros encargados sin contar con la autorización previa del responsable.

LA AEPD ACLARA

Videovigilancia y protección de datos personales (III): Grabación *on board*

En este informe emitido por el Gabinete Jurídico se analiza la conformidad de acuerdo con el RGPD y la LOPDGDD de los sistemas de captación y grabación de videocámaras instaladas en el exterior de vehículos o cascos de protección.

La finalidad de la grabación sería la obtención de una prueba para denunciar una posible infracción de las normas de tráfico.

En el informe, la AEPD valora que la legitimación podría ser el interés legítimo refiriéndose al derecho fundamental a la tutela judicial efectiva. Las fotografías o imágenes servirían como pruebas para denunciar infracciones a las normas de tráfico.

Cabe destacar que en este informe se hace referencia a otros anteriores en los que la AEPD determinó que, para la utilización de las cámaras *on board*, con esa finalidad concreta, se han de dar los siguientes criterios:

-Se utilizará solamente en los medios de transporte públicos y privados concesionarios de licencias para el transporte de personas.

-El sistema de grabación solamente se activará en caso de siniestro.

-La finalidad del tratamiento es legítima con la vinculación a la tutela judicial, queda excluido el uso de imágenes con fines de control laboral.

-La captación de imágenes hacia el exterior se limita al frontal del vehículo y hacia el interior excluyendo la imagen del conductor.

IMPORTANTE

Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia o sea imposible evitarlo.

ACTUALIDAD LOPD

La AEPD publica por primera vez el listado de Administraciones Públicas incumplidoras con sus requerimientos

Fuente: AEPD

(20 de abril de 2023). La Agencia Española de Protección de Datos (AEPD) ha publicado por primera vez la lista de las Administraciones Públicas sancionadas por incumplir los requerimientos y las medidas correctivas impuestas para garantizar el derecho fundamental a la protección de datos.

La lista está compuesta por Administraciones Públicas que **no cumplen con los requerimientos de información** remitidos por la Agencia, así como aquellas que no adecúan el tratamiento de datos a la legalidad y **no acreditan las medidas correctivas impuestas**. Tanto la falta de respuesta a los requerimientos como no acreditar que se han cumplido las medidas ordenadas para garantizar la protección de datos de los ciudadanos suponen infracciones clasificadas como muy graves.

Entre esas administraciones que no han cumplido las órdenes de la Agencia, destacan **entidades locales de más de 20.000 habitantes a las que se les ha requerido que nombren un Delegado de Protección de Datos (DPD)**. Al no cumplir con la orden remitida, la Agencia inicia un procedimiento sancionador contra estas administraciones por no atender el requerimiento de la Agencia.

La obligación de nombrar un DPD, establecida en el Reglamento General de Protección de Datos (RGPD) para autoridades u organismos públicos, supone disponer de un asesoramiento y supervisión especializada en materia de protección de datos, entre otras funciones, además de ofrecer una vía de contacto a los ciudadanos para que puedan obtener una respuesta adecuada a sus cuestiones. Transcurridos casi cinco años desde la aplicación del RGPD, aún son varias las entidades locales que siguen sin nombrar DPD y comunicar a la AEPD su designación, además de no cumplir con los requerimientos enviados. El nombramiento de Delegado de Protección de Datos y su comunicación a la Agencia suponen una obligación para las autoridades u organismos públicos incluida en el artículo 37 del Reglamento. La falta de cumplimiento supone una infracción calificada como grave.

De acuerdo con el artículo 77 de la Ley orgánica de Protección de Datos y garantía de los derechos digitales, la sanción que les corresponde es de apercibimiento.

Puede ver más información en el siguiente enlace:

Administraciones Públicas sancionadas por no responder a requerimientos y por incumplimiento de medidas

EL PROFESIONAL RESPONDE

¿Cómo pueden garantizar las normas de uso interno la ciberseguridad en mi empresa?

Para conseguir que nuestra empresa sea cibersegura tiene que haber una implicación de esta para la elaboración de las normas de uso interno en las que se abordan la ciberseguridad y el compromiso.

Todos los empleados/as han de estar informados de las políticas, normativas y buenas prácticas de la empresa. **Para garantizar la seguridad de la información en nuestra empresa se hace necesario desarrollar, entre otras, las siguientes políticas:**

- Política de protección de datos personales.
- Normas de uso de los dispositivos digitales.
- Política de seguridad en el puesto de trabajo.
- Política de almacenamiento (local, red corporativa, dispositivos externos y en la nube) y copias de seguridad.
- Política de gestión de soportes, borrado seguro y destrucción de la información.
- Política de control de acceso.
- Política de seguridad en la red.
- Política de trabajo fuera de los locales.

A esta normativa interna que desarrollamos a través de las políticas anteriores tenemos que añadir los procedimientos adecuados para que el perfil técnico de la empresa conozca como ejecutar las normas. Así por ejemplo para el control de acceso lógicos, se definirán las medidas de seguridad al dar de alta o baja a los usuarios de los sistemas.

IMPORTANTE

Las normas de uso interno han de estar a disposición del personal laboral. Se revisarán para adaptarlas a los cambios y nuevas necesidades de la empresa.