PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 07/19

EL RGPD UE 2016/679 EN APLICACIÓN

Elaboración de perfiles y toma de decisiones automatizada

Contenido

La elaboración de perfiles se define en el art.4 del RGPD, como **el tratamiento automatizado de datos personales**, con la finalidad de evaluar o analizar aspectos personales que permitan predecir el rendimiento profesional, la situación económica, la salud, preferencias o intereses personales, fiabilidad, comportamiento y la ubicación o movimientos de una persona.

Cuando la elaboración de perfiles, sea utilizada con la finalidad de tomar decisiones sobre una persona, basadas exclusivamente en un tratamiento automatizado, el interesado deberá ser informado previamente de la lógica aplicada y de la importancia de las consecuencias y efectos jurídicos que se produzcan en base a esa decisión. Además, tendrá derecho a oponerse a ese tratamiento, salvo que se den alguna de las siguientes circunstancias:

1º Que la decisión sea necesaria para la celebración o ejecución de un contrato entre el interesado y el responsable.

2º Esté autorizada por el Derecho de la Unión o los Estados miembros.

3º Que el interesado haya dado su consentimiento explícito.

IMPORTANTE

El responsable adoptará medidas adecuadas. Como mínimo, la intervención humana del responsable y el derecho a expresar su punto de vista e impugnar la decisión.

SANCIONES DE LA AEPD

Sanción a XFERA MÓVILES, S.A (YOIGO) por incluir de forma indebida a un cliente en un fichero de morosos

La AEPD ha dictado recientemente una resolución sancionando a la entidad YOIGO https://www.aepd.es/resoluciones/PS-00011-2019_ORI.pdf.

La reclamante DªAAA presentó un escrito ante la AEPD para reclamar que había sido incluida de forma indebida por YOIGO en un fichero de solvencia patrimonial y crédito Badexcug, a pesar de que el pago que le reclamaban había sido satisfecho en el plazo de los 15 días concedido, aportando en la reclamación el justificante de la transferencia de pago.

A la vista de los hechos y documentos presentados, la AEPD inicia un periodo de investigación y realiza un requerimiento informativo a YOIGO, el cual no contesta, **con lo que se le notifica el inicio del procedimiento sancionador, por infringir el principio de exactitud del art.5.1.d del RGPD, puesto que no actuó con la debida diligencia, al no verificar que la deuda informada al fichero de morosos era inexacta**. Las entidades que gestionan los ficheros de morosos suministran periódicamente, las relaciones de las altas y bajas, a las empresas informantes que son las que deciden la cancelación de los datos de sus clientes del fichero de morosidad.

En este caso YOIGO mantuvo la inscripción de la reclamante, después de haber realizado el pago de la deuda reclamada.

La sanción impuesta por la AEPD, después de aplicar los criterios de graduación, **asciende a la cantidad de 60.000 euros.**

Para un tratamiento lícito de estos datos personales, las deudas deben ser ciertas, vencidas y exigibles, que hayan sido facilitadas por el acreedor y éste le haya comunicado la inclusión en el fichero al interesado.

IMPORTANTE

No se incorporarán a los sistemas de información crediticia, las deudas en las que la cuantía principal sea inferior a 50 euros.

LA AEPD ACLARA

¿Se puede compartir información entre profesionales de distintos ámbitos y administraciones?

La AEPD en su informe da respuesta a varias consultas con un mismo hilo conductor, la protección de datos personales relativos a violencia de género.
https://www.aepd.es/media/informes/2018-0070-violencia-de-genero.pdf

Una de las consultas que se plantean es **si resulta conforme a la normativa en materia de protección de datos compartir información, entre distintos profesionales de distintos ámbitos y administraciones, para realizar la labor de seguimiento.** En este sentido, la legitimación la encontramos en la *ley 27/2003, reguladora de la orden de protección de las víctimas de violencia doméstica*, en la que se dice que: "en caso de adoptarse una orden de protección por el Juez, las Administraciones públicas tomarán medidas que garanticen la protección de seguridad o de asistencia social, jurídica, sanitaria, psicológica y para ello se **establecerá un sistema integrado de coordinación administrativa, que garantice la agilidad de las comunicaciones.**

Otra de las cuestiones planteadas se refería **al cumplimiento de los estándares de seguridad (nivel alto) en relación con el contenido y recorrido de los datos personales de las víctimas de violencia de género.** En este caso, la AEPD indica que, en el RGPD, no se establece un elenco de medidas de seguridad específicas, sino que, en virtud del principio de responsabilidad activa, **el responsable tendrá que determinar las medidas técnicas y organizativas concretas, en base al análisis de riesgos previamente realizado.**

IMPORTANTE

Las medidas de seguridad se aplicarán teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, contexto y fines del tratamiento.

ACTUALIDAD LOPD

La AEPD alerta a pymes y autónomos de los riesgos de contratar servicios de adecuación a la normativa a 'coste cero'

Fuente: https://www.aepd.es/prensa/2019-07-04.html

(3 de julio de 2019). La Agencia Española de Protección de Datos (AEPD) ha publicado un documento informativo en el que alerta a pymes y autónomos de los riesgos de contratar los servicios de adecuación a la normativa de protección de datos a empresas que la ofrecen a 'coste cero'. El documento, que ha sido elaborado con la colaboración de la Inspección de Trabajo y Seguridad Social y la Agencia Tributaria, también recoge otras prácticas fraudulentas que suelen estar asociadas a este tipo de servicios.

La adecuación a la normativa de protección de datos conocida como coste cero consiste en ofertar estos servicios a un precio muy bajo o incluso de forma gratuita, abonando el pago de estos mediante los fondos de la empresa destinados a los programas de formación para trabajadores, que son objeto de bonificación por parte de la Seguridad Social.

La contratación del servicio de adecuación a la normativa de protección de datos a coste cero, financiada con cargo a fondos públicos a través de bonificaciones en las cuotas a la Seguridad Social para la formación profesional para el empleo, puede derivar en infracciones que se sancionarán, por la Inspección de Trabajo y Seguridad Social, con multas de 626 euros a 187.515 euros, sin perjuicio de considerar, en cada caso, una infracción por cada empresa y por cada acción formativa, la solidaridad de los distintos sujetos intervinientes en la organización y ejecución de la formación en la devolución de las cantidades indebidamente obtenidas y las sanciones accesorias que en cada caso procedan.

Además, en lo referente al cumplimiento de obligaciones tributarias por parte de las empresas, tanto de quien oferta el servicio como de quien lo contrata, las actividades formativas destinadas a los trabajadores están exentas de tributación por el IVA, mientras que el tipo que corresponde a un servicio de adecuación a una determinada legislación sería del 21%. De enmascararse el servicio realmente llevado a cabo se puede estar cometiendo, por tanto, una infracción tributaria, sancionable con multa pecuniaria proporcional, del 50% en adelante, sobre la cuantía no ingresada.

La Agencia también advierte a pymes y autónomos, destinatarios fundamentales de este tipo de prácticas, que los servicios de adecuación a la normativa requieren de la realización de un estudio individual pormenorizado de la entidad, los tipos de tratamientos que se realizan, los sistemas informáticos y los sistemas de gestión documental, aplicando los principios de protección de datos en los procedimientos. Por tanto, es insuficiente un asesoramiento basado en documentos genéricos que no tengan en cuenta las características específicas de la actividad.

Puede ver más información en el siguiente enlace:

Adecuación a la normativa a coste cero y otras prácticas fraudulentas.

https://www.aepd.es/media/estudios/coste-cero.pdf

EL PROFESIONAL RESPONDE

¿Se tienen que realizar auditorías de seguridad y cumplimiento de la normativa de protección de datos?

El responsable y encargado del tratamiento deben ser proactivos y cumplir con la normativa de protección de datos, en este sentido una de las obligaciones que nos exige el reglamento es garantizar la seguridad de los datos personales.

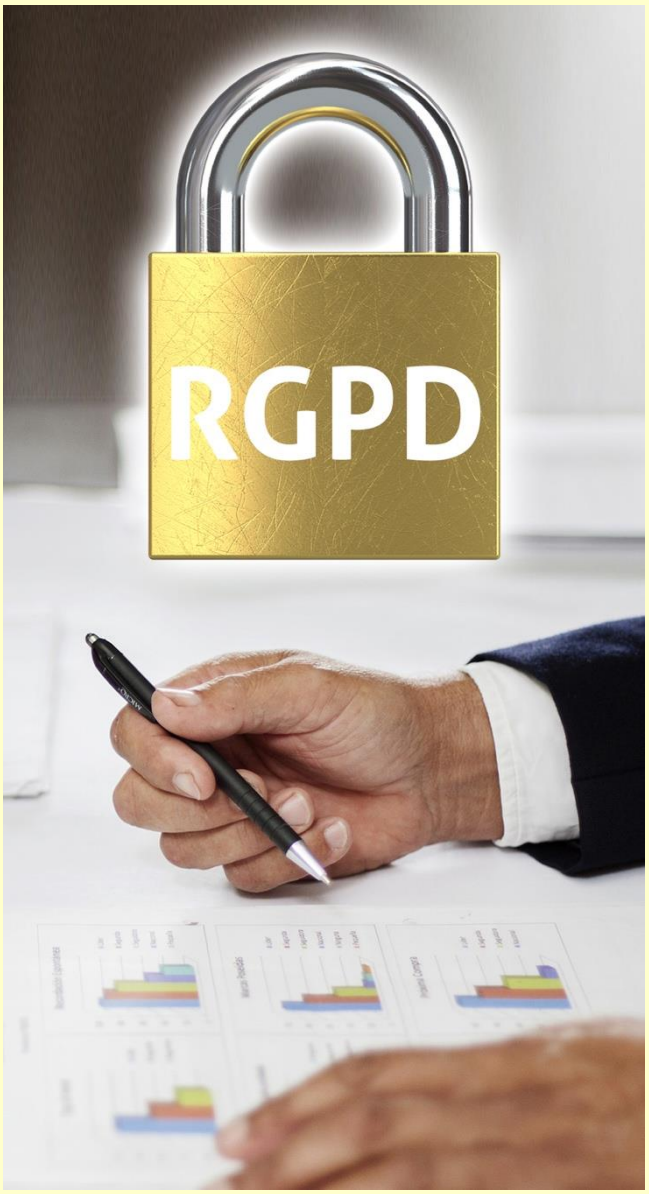
En el art.32 del RGPD se identifican algunas de las medidas técnicas y organizativas que el responsable y encargado del tratamiento deben aplicar para conseguir un nivel adecuado de seguridad, entre ellas:

32.1.d Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas.

En este sentido, el Reglamento se está **refiriendo a las auditorías como una de las medidas técnicas que se deben aplicar para salvaguardar la información.**

A lo largo del articulado del RGPD, también **se pueden encontrar otras referencias a las auditorías, cuando nos indica, en el art. 28 del RGPD,** que una de las cláusulas del contrato de acceso a datos por cuenta del responsable, el encargado del tratamiento permitirá y contribuirá a la realización de auditorías, incluidas las inspecciones por parte del responsable o incluso de otro auditor autorizado por dicho responsable.

Así mismo en el art.24 del RGPD, se recoge que el responsable aplicará las medidas adecuadas, con el fin de garantizar y demostrar que el tratamiento es conforme con el RGPD, dichas medidas se revisarán y actualizarán cuando sea necesario.



IMPORTANTE

"La falta de adopción de medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado, según el artículo 32.1 del Reglamento, es una falta grave.