PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 06/20

EL RGPD UE 2016/679 EN APLICACIÓN

Las auditorías de protección de datos

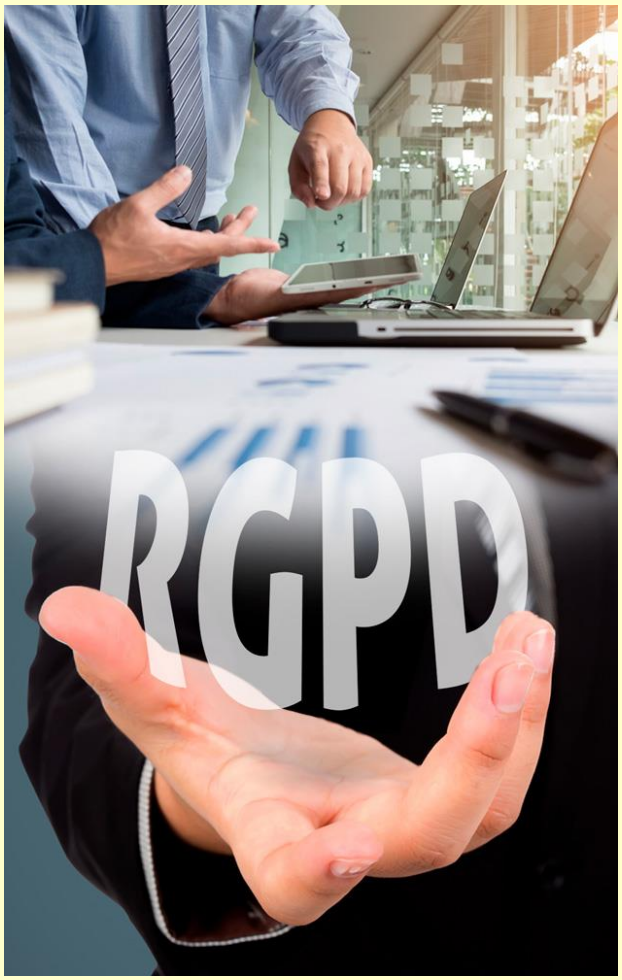
Una de las principales características de la aplicación del RGPD es que es el propio responsable, mediante un minucioso análisis de riesgos, el que determina cuáles son las medidas técnicas y organizativas más apropiadas para el tratamiento que se lleva a cabo en su entidad.

En el art.32 del RGPD se indican como mínimo algunas de las medidas que se deben aplicar para garantizar la confidencialidad, disponibilidad e integridad de la información. **En concreto, se menciona a la auditoría de protección de datos como "un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento".**

En la anterior normativa se establecía un plazo para su realización dependiendo del nivel de seguridad bajo, medio o alto. En la actualidad como estos plazos no se encuentran regulados por la ley, será el responsable el que en función del análisis de riesgos establezca la periodicidad para su realización.

No solamente será obligación del responsable, también el encargado del tratamiento. Este tiene que poner a disposición del responsable para permitirle la realización de auditorías, incluidas las inspecciones, por parte del responsable o auditor autorizado.

Contenido



IMPORTANTE

Uno de los cometidos de los delegados de protección de datos es la supervisión del cumplimiento del RGPD, incluidas las auditorías.

SANCIONES DE LA AEPD

Primera sanción a una entidad por no tener nombrado un Delegado de Protección de Datos

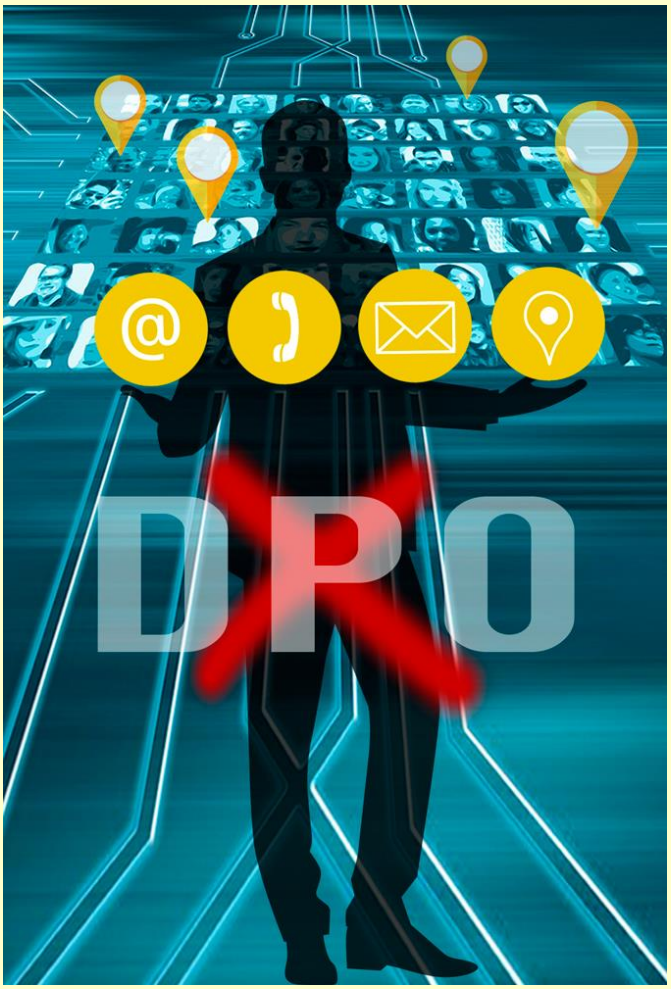
En el reciente procedimiento sancionador https://www.aepd.es/es/documento/ps-00417-2019.pdf instruido por la AEPD, se sanciona a la entidad GLOVOAPP23, (en adelante el reclamado) por no tener designado un Delegado de Protección de Datos (en adelante DPD).

Está aumentando la conciencia de los usuarios respecto de la protección de sus datos personales, cada vez se preocupan más por conocer qué hacen los responsables con sus datos y cómo ejercer sus derechos reconocidos en el RGPD y LOPDGDD. **Este es el caso de dos reclamantes que se dirigieron a la AEPD para poner en su conocimiento, que la entidad GLOVO no tenía nombrado un DPD al que dirigir las reclamaciones.**

La AEPD en virtud de su potestad investigadora solicitó a la reclamada que presentara las alegaciones oportunas. La entidad, en su escrito de contestación a la reclamación, alegaba que había constituido un Comité de Protección de Datos que realizaba las funciones propias de un DPD, además, indicaba en ese escrito, que su actividad no estaba incluida dentro de los supuestos de designación obligatoria de DPD.

Finalmente, la AEPD determina en su resolución que la reclamada está obligada a nombrar un DPD, puesto que lleva a cabo un tratamiento de datos habitual y sistemático de interesados, considerado a gran escala. **Es la primera sanción de este tipo y alcanza la cuantía de 25.000 euros.**

El incumplimiento de designar un DPD cuando sea exigible su nombramiento se considera en nuestra LOPDGDD una infracción grave.



IMPORTANTE

Los agravantes de la sanción fueron el tratamiento de datos personales a gran escala y el tipo de datos afectados.

LA AEPD ACLARA

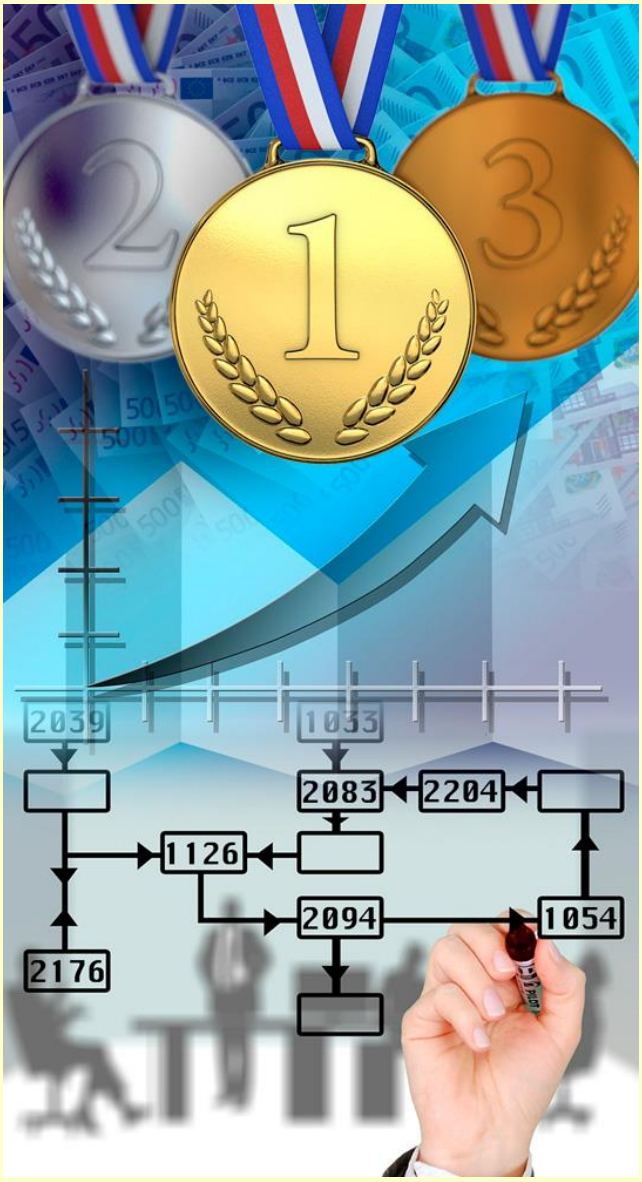
¿Es legal publicar en un tablón de la empresa un listado de productividad de los empleados/as?

La consulta es planteada a la AEPD https://www.aepd.es/es/documento/2018-0183.pdf por una entidad que se dedica a la comercialización de productos derivados del cerdo ibérico puro (con un alto valor económico).**El responsable de la empresa pretende publicar semanalmente en el tablón de anuncios existentes en la sala de deshuesado, la productividad de cada persona según el número de sobres de jamón/paleta loncheado que hayan realizado.**

Al final de mes el Departamento de Recursos Humanos pagará una prima de productividad. El objetivo de la publicación es generar una competitividad sana entre los empleados/as y, además, transparencia en la obtención de la prima.

Ante este planteamiento, la AEPD estima que la publicación de esos datos que consiste en el número de matrícula (dato conocido por el propio trabajador/a y el Departamento de Recursos Humanos) estaría legitimado en el interés legítimo del responsable (art.6.1. f del RGPD), que consiste en generar una competitividad sana que ayude a mejorar la productividad general. **También hace referencia al interés legítimo del personal laboral, puesto que pueden conocer su propio rendimiento y se garantiza la transparencia en la obtención de la prima económica.**

La AEPD da unas pautas para su publicación recomendando que se haga solamente en el tablón de anuncios de la Sala en la que se desarrolla la actividad laboral.



IMPORTANTE

Siempre que la legitimación del tratamiento sea el Interés legítimo del responsable o de un tercero se debe hacer un Juicio de Ponderación.

ACTUALIDAD LOPD

La AEPD analiza por primera vez el cumplimiento de la protección de datos en el ámbito de la atención sociosanitaria

Fuente: AEPD

(Madrid, 1 de junio de 2020). La Agencia Española de Protección de Datos (AEPD) ha publicado el 'Plan de Inspección de oficio de la atención sociosanitaria', que analiza por primera vez los tratamientos que se llevan a cabo en este ámbito e investiga su adecuación a la normativa de protección de datos.

Las inspecciones de oficio que realiza la Agencia en distintos sectores o áreas específicas **no tienen carácter sancionador sino preventivo** y se llevan a cabo para obtener una visión integral que permita detectar deficiencias y realizar las oportunas recomendaciones. La finalidad de estas inspecciones es elevar el nivel de protección de los ciudadanos a través del análisis de los datos que manejan las organizaciones.

El plan contiene conclusiones respecto del cumplimiento del Reglamento General de Protección de Datos (RGPD) y de la Ley Orgánica de Protección de Datos y garantía de los derechos digitales (LOPDGDD), así como **recomendaciones dirigidas a organismos públicos, empresas e instituciones titulares de centros sociosanitarios**, que inciden en actuaciones necesarias para una correcta aplicación de la normativa. También incluye un decálogo que resume las principales conclusiones y un grupo de preguntas y respuestas frecuentes con las dudas recogidas durante su ejecución.

Entre las conclusiones más relevantes se encuentran las referidas a la **información que se debe ofrecer al usuario de estos servicios, que preferiblemente será por capas**, concisa y con un lenguaje claro, de acuerdo con la capacidad de comprensión del destinatario de la información. Por ejemplo, la primera capa deberían ser carteles informativos sencillos ubicados en zonas de acceso a los centros, en los que se podrían incluir referencias a otras capas de información más detallada.

Durante las auditorías se detectaron problemas relacionados con la identificación por parte de los responsables de las bases jurídicas que amparan los tratamientos, por lo que la Agencia recuerda que para cada actividad de tratamiento realizada hay que identificar su base jurídica.

El apartado de preguntas frecuentes da respuesta a otras dudas surgidas en el contexto de la actividad de la atención sociosanitaria, por ejemplo, si es posible cancelar determinados datos de un usuario a petición suya, llevar a cabo tratamientos con fines de investigación médica en un centro, o si es obligatorio facilitar datos personales de los usuarios del centro si lo solicitan las fuerzas de seguridad.

Puede ver más información en los siguientes enlaces

Plan de Inspección de oficio de la atención sociosanitaria

EL PROFESIONAL RESPONDE

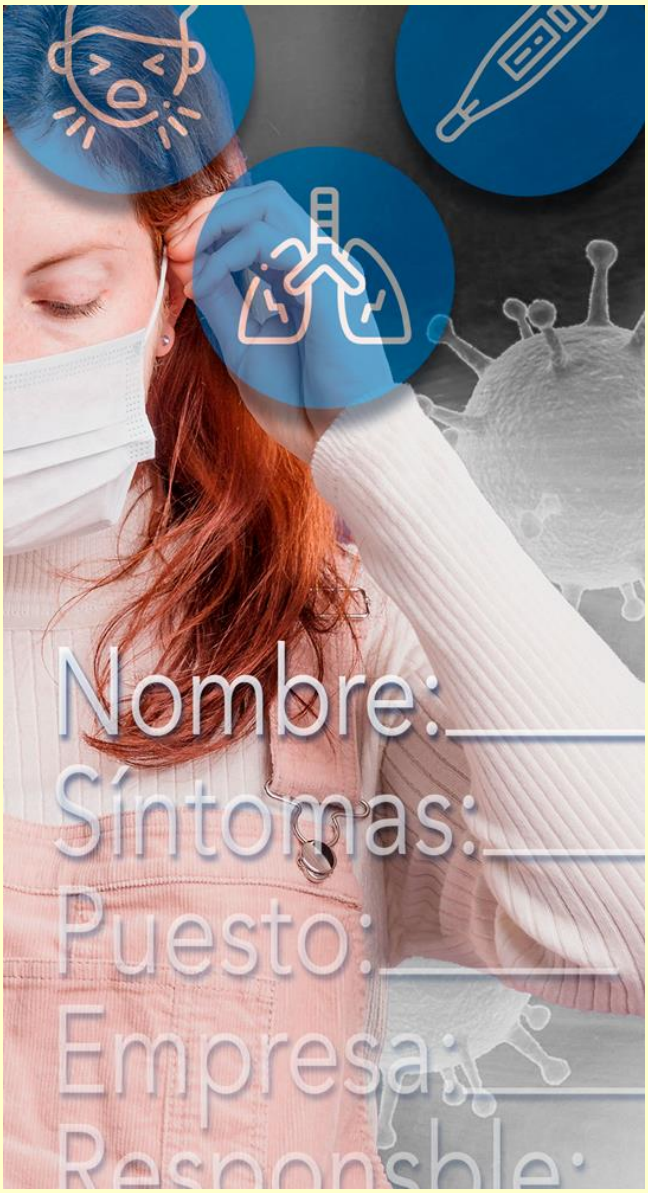
¿Podríamos difundir la identificación de un trabajador/a afectado por el COVID-19?

A lo largo de la evolución de la pandemia originada por el Covid-19 han surgido muchas dudas acerca del tratamiento de los datos personales relacionados con la salud de los trabajadores/as de las empresas.

El responsable de la entidad, en aplicación de la normativa de prevención de riesgos laborales, debe garantizar la seguridad y la salud de su centro de trabajo, para ello aplicará las medidas adecuadas al nivel de riesgo de su entidad, que vengan determinadas por los servicios de prevención de riesgos laborales y de la salud. **En el caso de que uno de los trabajadores/as estuviera afectado por el virus, su identificación personal, solamente se realizará a las autoridades competentes, en concreto a las sanitarias.**

La AEPD, en su apartado de consultas frecuentes, indica que en el caso de que no sea posible cumplir con el objetivo de garantizar la seguridad en el centro de trabajo sin identificar al afectado/a, se podrá proporcionar esa información identificativa.

Por otro lado, el personal laboral que se encuentre en alguna de estas situaciones, que presenten síntomas compatibles con Covid-19 o estén en aislamiento domiciliario o bien hayan tenido contacto estrecho con alguna persona infectada, deberán ponerlo en conocimiento del responsable.



IMPORTANTE

Se tienen que tratar los datos observando los principios del RGPD, en particular minimización, limitación y criterios de conservación mínimos.