PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 03/22

EL RGPD UE 2016/679 EN APLICACIÓN

Deber de secreto y seguridad en el ámbito laboral (II)

Dos de los principios fundamentales en el tratamiento de los datos en el ámbito laboral son el deber de secreto y seguridad. El responsable en el ejercicio de sus actividades debe garantizar el secreto y la seguridad en el tratamiento de los datos personales, y, además, debe demostrarlo. Por ello, se hace necesario que se apliquen medidas técnicas y organizativas imprescindibles.

Algunas de estas medidas podrían ser las enumeradas a continuación:

- Diseñar funciones y responsabilidades de la plantilla de personal.
- Formar adecuadamente a las personas trabajadoras según el grado de responsabilidad que contribuya a crear una cultura de compromiso con la protección de datos.
- Advertir y formar, inclusive, los perfiles que no tienen relación directa con el tratamiento de datos personales.
- Valorar la designación de un delegado de protección de datos, con expertos formados en la materia, que asesoren en el cumplimiento de la normativa y el principio de responsabilidad proactiva.

El incumplimiento del deber de secreto y seguridad suponen graves perjuicios para la empresa y su reputación.

Contenido

IMPORTANTE

La falta de adopción de medidas técnicas y organizativas para aplicar los principios de protección de datos supone una sanción grave.

SANCIONES DE LA AEPD

Una empresa de educación es sancionada con 9.000 euros por publicar imágenes de su personal laboral en RRSS

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00119-2021.pdf, se sanciona a una empresa dedicada a prestar servicios de educación por la publicación de imágenes de su personal laboral en las redes sociales y en la página web corporativa.

El reclamante, en su escrito, aporta copia de los correos que envió a la dirección web del reclamado para que retirara sus fotos de la página web y redes sociales. También envía un archivo con fotografías web bajo el rótulo de "Equipo educativo".

La AEPD inicia el procedimiento sancionador ya que la empresa a incumplido lo dispuesto en el RGPD.

Por un lado, la reclamada no tenía legitimación para el tratamiento de los datos personales del afectado, puesto que, para la publicación de imágenes del personal laboral en la página web de la empresa y RRSS se requiere el consentimiento expreso de los trabajadores/as. **La relación laboral no legitima al responsable para la publicación de imágenes.**

Además, el responsable no respondió al derecho de supresión solicitado por el reclamante, hasta en dos ocasiones, tal y como consta en el escrito de reclamación.

La multa ascendió a un total de **9.000 euros.**

El responsable debe aplicar medidas de seguridad que garanticen la confidencialidad de los datos.

IMPORTANTE

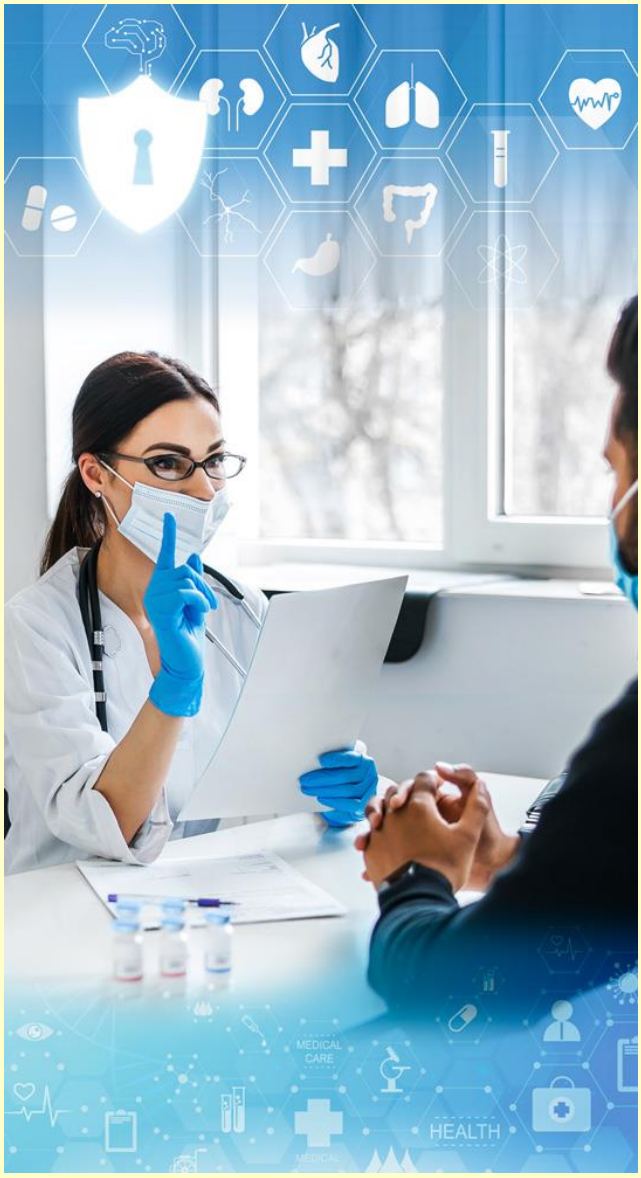
La publicación de imágenes se considera una cesión a terceros por lo que debe ser debidamente informada y legitimada por el responsable de los datos.

LA AEPD ACLARA

Plan de Inspección de Oficio de la Atención Sociosanitaria (III) Información ofrecida al usuario

En el apartado de la AEPD Guías y Herramientas, encontramos el documento denominado "Plan de Inspección de Oficio de la Atención Sociosanitaria"

En este plan de inspección de Oficio, la AEPD analiza la información que se le ofrece al usuario en materia de protección de datos. **Las conclusiones a la que ha llegado, entre otras, es que en la mayoría de los centros auditados carecen de carteles informativos en las zonas de recepción o en otras zonas de acceso de los pacientes. Además, se ha detectado que existían carteles desactualizados con referencia a la normativa antigua.** En los formularios adaptados al RGPD se evidencia cierta confusión cuando se informa de la base jurídica o licitud.



La AEPD da una serie de recomendaciones para solventar las deficiencias analizadas:

- Colocación de carteles informativos sencillos, actualizados y de fácil lectura para los usuarios, en las zonas de acceso al centro.
- Informar siempre en el momento de la recogida de los datos y no en el momento del ingreso u otro posterior.
- La segunda capa de información debe ser consultada por el usuario inmediatamente de forma sencilla ya sea a su solicitud o por consulta on-line.
- Facilitar una copia al usuario cuando se utilice un solo documento informativo que sea firmado por el usuario para dejar acreditada la información facilitada.

IMPORTANTE

La información facilitada al usuario debe ser accesible a los usuarios, utilizando un lenguaje claro y sencillo.

ACTUALIDAD LOPD

La AEPD publica una lista de verificación para ayudar a los responsables a realizar evaluaciones de impacto

Fuente: AEPD

(Madrid, 17 de febrero de 2022). La Agencia Española de Protección de Datos (AEPD) ha publicado una lista de verificación para ayudar a los responsables del tratamiento a identificar y determinar de una forma rápida si el proceso y la documentación que están siguiendo para llevar a cabo una Evaluación de Impacto en la Protección de Datos (EIPD) contiene **los elementos exigibles**.

La AEPD cuenta con la guía 'Gestión del riesgo y evaluación de impacto en tratamientos de datos personales', que facilita la obligatoria gestión de riesgos en los procesos de gobernanza de las entidades y, cuando corresponda, la EIPD. **Este listado de verificación complementa esa guía** y permite, una vez desarrollada y documentada la Evaluación de Impacto, **efectuar una comprobación final** para cerciorarse de que se han tenido en cuenta todos los aspectos recogidos en la normativa de protección de datos.

El Reglamento General de Protección de Datos establece que las organizaciones que tratan datos personales deben realizar una gestión del riesgo con el fin de **establecer medidas para garantizar los derechos y libertades de las personas**. Además, en aquellos casos en los que los tratamientos impliquen un riesgo alto para la protección de datos, el Reglamento dispone que esas organizaciones están obligadas a realizar una Evaluación de Impacto en Protección de Datos para mitigar esos riesgos. Si tras la realización de la EIPD, y después de haber adoptado medidas, el riesgo sigue siendo alto, el responsable debe llevar a cabo una consulta previa a la autoridad de control antes de realizar ese tratamiento de datos personales.

El objetivo de este nuevo recurso de la AEPD es ayudar a los responsables a cumplir con las obligaciones de desarrollar y documentar una EIPD y para que, en caso de tener que realizar esa consulta previa a la Agencia, sea más sencillo comprobar que se cumple con los requisitos para su presentación, en particular los que se derivan de la Instrucción 1/2021, por la que se establecen directrices respecto de la función consultiva de la Agencia.

En este sentido, en caso de que los responsables del tratamiento tengan previsto realizar una consulta previa, la Instrucción 1/2021 establece que estos deberán contemplar lo señalado por la AEPD en sus guías y recomendaciones. En consecuencia, **el responsable deberá presentar esta lista de verificación cumplimentada** ante la Agencia, con el fin de incluir el contenido mínimo exigido y dotar a su consulta de mayor precisión y exactitud.

Puede ver más información en el siguiente enlace

Gestión del riesgo y evaluación de impacto en tratamientos de datos personales

EL PROFESIONAL RESPONDE

Garantizar la seguridad de la información con la implementación de medidas

Recientemente, el Tribunal Supremo ha dictado una sentencia relevante para la seguridad de los datos personales.

En este sentido, el Tribunal Supremo manifiesta que la obligación del responsable por mantener la seguridad de los datos es una obligación de medios y no de resultados. Es decir, a la hora de exigir responsabilidades, no puede hacerse sobre el hecho ya producido, sino sobre la diligencia de la implementación de las medidas.

Como responsables de la seguridad de la información tenemos que aplicar las medidas de seguridad en nuestra entidad teniendo en cuenta dos fases:

A) Análisis de la adecuación de medidas: En esta fase verificaremos que las medidas se ajustan al análisis de riesgos previo, que en la selección de medidas se han tenido en cuenta la probabilidad y el impacto de los riesgos identificados y en esta primera fase, además, comprobaremos que las medidas se han implantado de forma completa.

B) Análisis de la efectiva aplicación de las medidas: en esta segunda fase verificamos que las medidas se han implantado de forma completa, que están activas y siguen siendo las idóneas y que con su implantación evitan razonablemente las brechas de seguridad que puedan producirse.

IMPORTANTE

No basta con diseñar medios técnicos y organizativos necesarios, se hace imprescindible su correcta implementación y utilización.