PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 01/22

EL RGPD UE 2016/679 EN APLICACIÓN

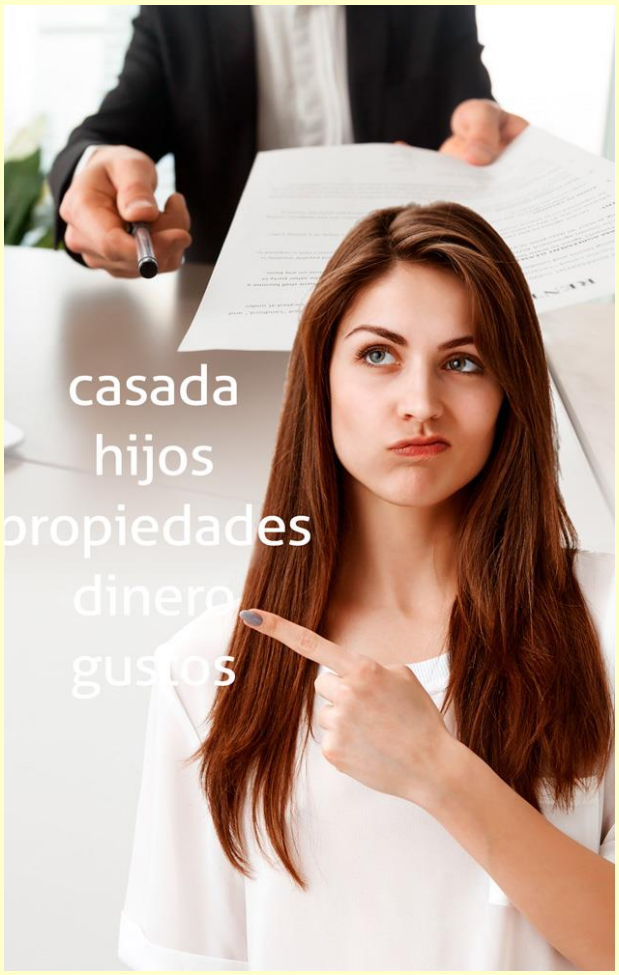
El principio de minimización y las relaciones laborales

Uno de los principios que debemos tener en cuenta cuando tratamos datos personales es la minimización de los datos (art 5.c RGPD). **Este principio nos obliga como responsables del tratamiento que los datos personales sean adecuados, pertinentes y limitados a lo necesario para los fines objeto del tratamiento.**

Los datos personales necesarios para el desarrollo de la relación laboral, podrían ser los siguientes, y a título solamente ejemplificativo, (según la guía de la AEPD): el nombre y apellidos de la persona trabajadora; sexo; número de DNI; número de afiliación de extranjero y de la Seguridad Social; nacionalidad; discapacidad y fecha de nacimiento.

Otros datos personales que no resultan imprescindibles para la ejecución de un contrato, se podrían tratar por el empleador con una base jurídica diferente a la del contrato, como podría ser el interés legítimo. Para ello, habría que analizar las características de cada relación laboral. Así, por ejemplo, la dirección de correo electrónico o el número de teléfono personal, son datos que permiten a la empresa localizar a su personal y contactar con ellos en caso necesario. El tratamiento será preciso ponderarlo caso por caso.

Contenido



IMPORTANTE

El interés legítimo se tiene que demostrar debidamente aplicando los principios de ponderación y proporcionalidad.

SANCIONES DE LA AEPD

Sanción de 50.000€ a una constructora por una cesión ilícita de datos de salud de un trabajador

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00324-2021.pdf, una empresa constructora es sancionada por ceder datos de salud (bajas médicas, motivos y permisos) a otra empresa, así como la dirección del correo personal, sin el consentimiento del trabajador (reclamante).

La entidad sancionada manifiesta que envió la documentación referida, por requerimiento de la Entidad Pública Empresarial de Vivienda, para defenderse de las denuncias interpuestas por el reclamante por falta de adscripción de medios humanos y materiales en la obra en la que se encontraba trabajando.

En este sentido, la AEPD considera que se ha vulnerado el art 5.1.c del RGPD "Principio de minimización de datos". Se están tratando datos de salud (bajas y permisos por COVID) y datos de carácter personal (correo electrónico personal del trabajador) para una finalidad distinta a la de servir como medio de comunicación entre empresa y trabajador. **Los datos que la entidad reclamada ha aportado como alegaciones para su defensa se consideran excesivos.**

En calidad de agravantes, se estima el tratamiento de los datos de salud, como categorías especiales de datos. La multa que se le ha impuesto ascendió a la cantidad de 50.000€.

Principio de minimización de datos: los datos han de ser adecuados, pertinentes y limitados a lo necesario en relación con los fines de su tratamiento

IMPORTANTE

El responsable debe realizar un tratamiento de datos de categorías especiales conforme a las excepciones dispuestas en el RGPD.

LA AEPD ACLARA

Plan de Inspección de Oficio de la Atención Sociosanitaria (I) Historia sociosanitaria y documentación

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

En este boletín y los siguientes analizaremos las recomendaciones más relevantes detalladas en este documento. **La AEPD analizó diferentes centros públicos y privados que prestan servicios sociosanitarios con atención directa a usuarios, siendo de ámbito estatal, regional y local y de diferentes tamaños. A lo largo del documento se recomiendan acciones de mejora.**

En el apartado de "Historia sociosanitaria y documentación", tras analizar la situación del tratamiento de los historiales sociosanitarios por parte de los centros auditados, se recomiendan las siguientes acciones:

-evitar la dispersión de documentos por diferentes departamentos, copias duplicadas, etc.: supone un riesgo en la integridad de la documentación al no poder realizar una actualización de la información adecuada.

- **digitalización total de la historia sociosanitaria del centro**: lo que permite acceder a ellas según las necesidades de los diferentes profesionales.

- **incluir registro de acceso**: cuando la digitalización no fuera posible, se instaurará un procedimiento de gestión de la documentación en papel, que incluya un registro de los accesos, para conocer en todo momento la trazabilidad de los datos personales.

IMPORTANTE
Crear procedimientos seguros para el traslado de la documentación sociosanitaria y aplicar una política de mesas limpias para evitar un acceso no autorizado de terceras personas.

ACTUALIDAD LOPD

Cifrado y Privacidad (V): la clave como dato personal

Fuente: AEPD

A la hora de aplicar criptografía, el uso de una clave es el parámetro determinante. Hay muchas definiciones de qué es una clave. Brevemente, podemos decir que una clave es un parámetro que determina el resultado de un algoritmo criptográfico. Atendiendo a la clave, los sistemas de cifrado se pueden dividir en dos grandes grupos: los cifrados simétricos, donde una única clave cifra y descifra; y los cifrados asimétricos, en los que se precisan de dos claves, una para cifrar, que puede tener carácter público, y otra, para descifrar, que tiene carácter privado y está únicamente en posesión de su legítimo titular. Las dos claves del cifrado asimétrico están vinculadas, pero es muy difícil deducir una de la otra si no se dispone de información adicional.

Los cifrados asimétricos están diseñados para que una de las claves se desvele y sea de libre acceso, la clave pública, por lo que son muy adecuados para su empleo en Internet. De esta forma, el uso de las claves asimétricas no solo permite el cifrado/descifrado de información, sino también realizar la autenticación de personas, la generación o la verificación de firmas, el intercambio de claves simétricas, etc.

Las claves públicas pueden ser empleadas por personas, entidades e incluso máquinas para identificarse, autenticarse o intercambiar información. Cuando se trata de claves públicas que corresponden a personas físicas cabría plantearse si estas claves se pueden considerar datos de carácter personal. A este respecto, tanto la autoridad francesa CNIL (Solutions for a responsible use of the blockchain in the context of personal data) como el Parlamento Europeo (Blockchain and the General Data Protection Regulation) ya han manifestado que son datos personales en el marco de tratamientos específicos.

Para determinar la naturaleza de datos de carácter personal de la clave pública hay que tener en consideración la propia definición de dato personal establecida en el artículo 4:

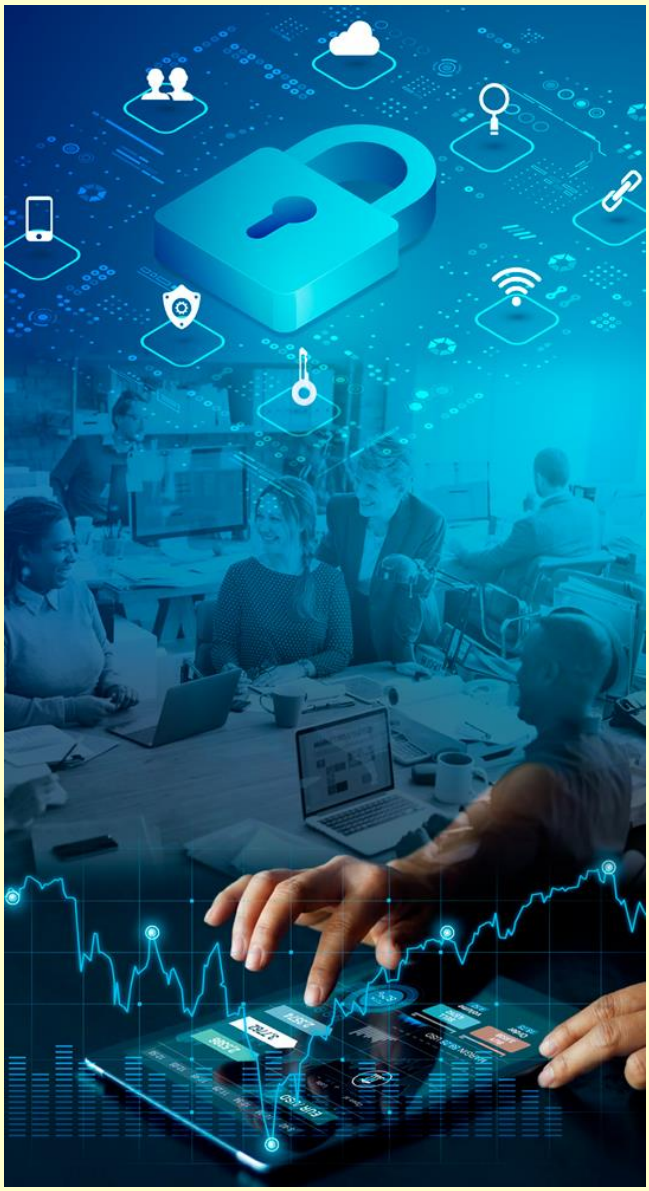
«datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona

Puede ver más información en el siguiente enlace

Innovación y Tecnología

EL PROFESIONAL RESPONDE

Cómo proteger la seguridad de la información en la empresa



En este apartado "El profesional responde", iremos abordando la importancia de conocer y desarrollar procedimientos para mantener la seguridad de la información de nuestra empresa.

Lo primero que tenemos que definir es el concepto de seguridad de la información. Todas las empresas independientemente de su tamaño tienen que proteger su información para poder seguir creciendo y cumpliendo sus objetivos profesionales. Así, por ejemplo, debemos aplicar medidas para garantizar la confidencialidad de los datos bancarios de nuestros clientes o la propiedad intelectual de nuestra empresa o las tarifas y ofertas que nos posicionan en el mercado.

Estos son algunos de los principales errores que se cometen en el tratamiento de la información y que ponen en peligro la seguridad de la información:

-carpetas de red compartidas sin control de acceso.

-Usuarios que aún conservan acceso a información que ya no es necesaria en su nueva posición en la empresa.

-Eliminar los ordenadores y discos sin analizar su contenido y eliminar la información confidencial.

-No realizar copias de seguridad de la información y asegurarnos que tenemos una copia de seguridad actualizada.

IMPORTANTE

Las empresas independientemente de su tamaño deben evitar riesgos en su activo vital más importante: la información.