PRODASUR
Consultores en Protección de Datos (RGPD-LOPD)

RGPD-LOPD
en la empresa

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

Boletín 09/21

EL RGPD UE 2016/679 EN APLICACIÓN

Derechos digitales en el ámbito laboral. Derecho a la intimidad

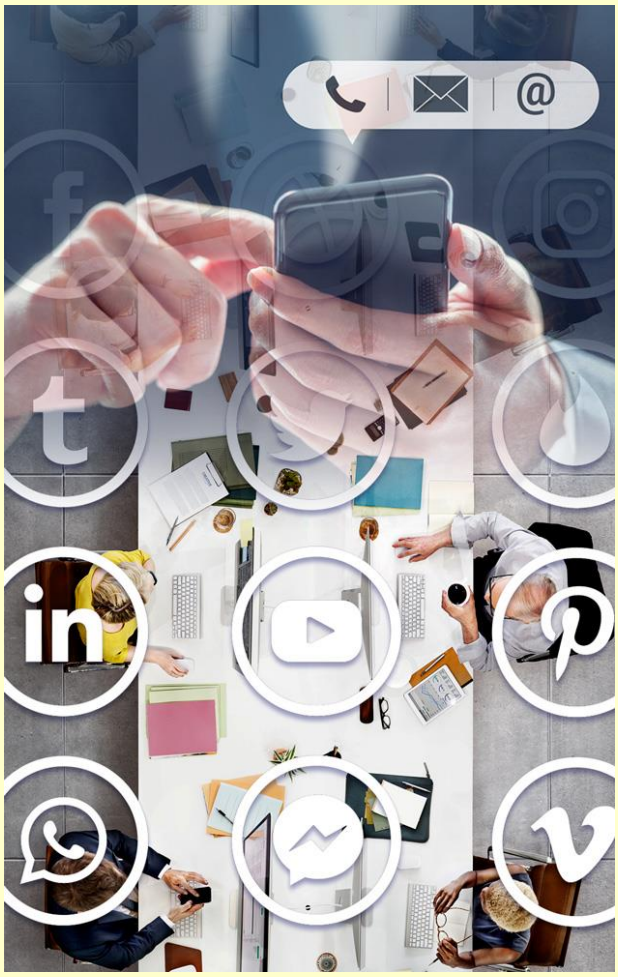
Contenido

En el entorno laboral, los responsables del tratamiento, en este caso, los empleadores, deben de garantizar a todo el personal laboral la protección de su intimidad en el uso de los dispositivos digitales. Así viene regulado en el art.87 de la LOPDGDD

Hoy en día, en el que estamos inmersos en la era de la digitalización, muchas de nuestras actividades laborales se desarrollan utilizando todo tipo de dispositivos digitales, tales como ordenadores portátiles, tabletas, teléfonos inteligentes y *wearables*. Se hace necesario que los empleadores establezcan criterios claros de utilización de estos dispositivos digitales según los usos sociales y los derechos reconocidos constitucionalmente.

A través de las políticas de utilización de dispositivos digitales, que toda empresa debería tener actualizada y revisada, se podría facilitar la información al personal laboral a cerca de los criterios de utilización. Facilitar esta información es un deber a cumplir por parte de la empresa.

El empleador podrá acceder al contenido derivado del uso de esos dispositivos digitales. La finalidad será el control del cumplimiento de las obligaciones laborales o estatutarias y garantizar la integridad de los dispositivos digitales.



IMPORTANTE

Cuando en los dispositivos digitales se permita un uso con fines privados se establecerán claramente los periodos de uso como garantía de la privacidad de la persona trabajadora.

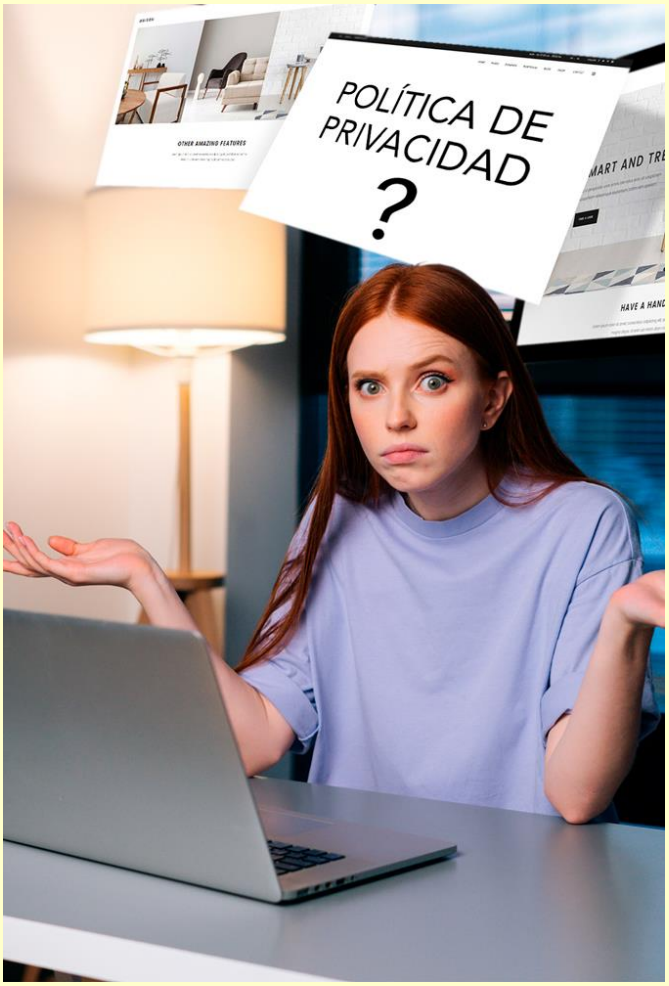
SANCIONES DE LA AEPD

Una página web es sancionada con 10.000 euros por no incluir la política de privacidad adecuada al RGPD

En la resolución de la AEPD https://www.aepd.es/es/documento/ps-00251-2021.pdf, se sanciona a una página web por no informar debidamente a sus usuarios en la política de privacidad.

La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales es una infracción calificada en nuestra LOPDGDD como muy grave.

La AEPD inicia el procedimiento sancionador por la reclamación presentada por una persona al fijarse que la página web visitada no tenía una política de privacidad adecuada a la normativa de protección de datos.



En concreto, la afectada indica que al querer enviar una reclamación al titular de la web no había modo alguno de realizarlo, puesto que no existía teléfono y el email facilitado no funcionaba correctamente ya que devolvía los correos enviados. La reclamante facilita en su escrito de reclamación una copia a la AEPD de los textos legales que se encuentran en la página. **Estos textos hacían referencia a la antigua ley de protección de datos.**

Los formularios de la página web sancionada incluían la recogida de datos personales incluidos en su caso datos bancarios.

La AEPD determina que no se proporciona una información clara y adecuada al usuario. Además, se tienen en cuenta como agravantes, la negligencia en la infracción, la forma en que la AEPD conoce la infracción a través de una reclamación y por ultimo la falta de cooperación con la AEPD para poner remedio a la situación. **La multa ascendió a un total de 10.000 euros.**

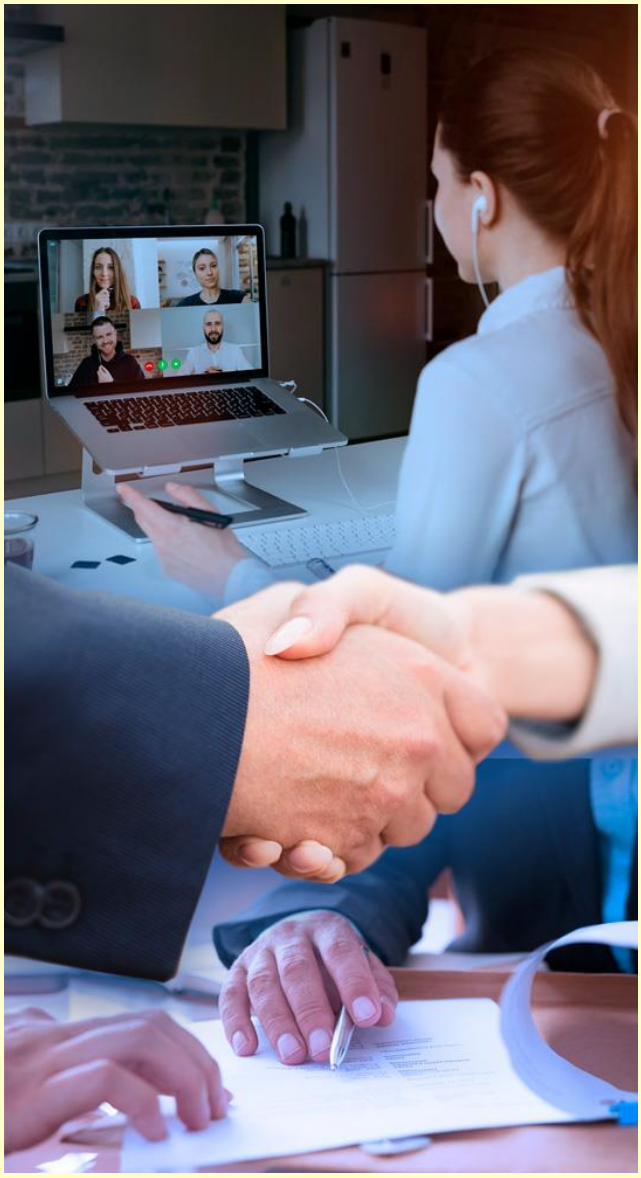
IMPORTANTE

Las páginas web que contengan formularios deben incluir políticas de privacidad claras, concisas y conforme al RGPD.

LA AEPD ACLARA

Teletrabajo y protección de datos en el ámbito digital

La AEPD ha publicado en su apartado de prensa y comunicación el resumen de las claves a tener en cuenta para garantizar la protección de los datos personales de las personas trabajadoras que realizan teletrabajo como de los datos de los clientes y proveedores.



En el artículo, la AEPD deja evidencia que lo que se presuponía temporal se ha quedado, al menos, en buena parte de las entidades. Se está desarrollando un nuevo modelo económico que forma parte de la digitalización. **Las soluciones que se tomaron durante el comienzo de la pandemia deben ser revisadas, ya que en muchos casos se aplicaron con urgencia y a corto plazo.**

En lo que respecta al tratamiento de los datos de las personas trabajadoras que realizan teletrabajo, hay que considerar la voluntariedad del trabajo a distancia. **El consentimiento no se aplicará como base legítima puesto que la persona trabajadora está en una situación de desigualdad respecto de la empresa.** Hay que buscar otras legitimaciones adecuadas como el cumplimiento de obligaciones legales por parte de la entidad recogidas, por ejemplo, en el Estatuto de los trabajadores o en el RD- ley de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo.

Se hace mención al derecho a la intimidad, al uso de los dispositivos digitales y al derecho a la desconexión digital en el ámbito laboral.

IMPORTANTE

Es obligatorio la firma del acuerdo de trabajo a distancia que incorpora la Ley 10/2021, de 9 de julio, de trabajo a distancia.

ACTUALIDAD LOPD

¿Quién es el responsable del tratamiento de los datos en un centro educativo? ¿Para qué recurrir al Delegado de Protección de Datos?

Fuente: AEPD

La Agencia Española de Protección de Datos (AEPD) ha desarrollado en los últimos años un amplio abanico de iniciativas relacionadas con la educación y los menores. Además, dispone de un servicio llamado Canal Joven, que ofrece varias vías de comunicación dirigidas a dar respuesta a las cuestiones o dudas relacionadas con el ámbito escolar.

Por otro lado, la AEPD publica habitualmente documentos sencillos como complemento a la información facilitada a través de sus canales. Todas ellos están disponibles en una sección específica de la página web de la Agencia y, aunque abordan en su mayoría temas que ya han sido tratados en formatos como guías u otros documentos más extensos, desde la Agencia se considera que estos documentos simplificados pueden ayudar de una forma más directa tanto a los ciudadanos como a los responsables.

En este sentido, la Agencia ha publicado una nueva infografía que recoge las **diferentes figuras implicadas en el tratamiento de datos en los centros educativos**: interesado/a, responsable del tratamiento de datos, encargado/a del tratamiento y delegado/a de protección de datos.

En los nueve primeros meses de este año, **el Canal Joven ha recibido más de 1.200 consultas**, lo que, a falta de un trimestre para concluir el año, supone casi haber alcanzado la cifra de 2020. Dado el número de preguntas recibidas que inciden en la responsabilidad de los tratamientos de datos en los colegios y qué hacer cuando plantean dudas o controversias al respecto, la Agencia clarifica en esta infografía de quién son los datos que tratan los centros educativos (alumnado, profesorado, personal de servicios, etc.), quién es el responsable de su tratamiento en cada caso, quién gestiona los datos personales atendiendo al encargo que le hace el responsable, y quién tiene la función de asesorar para que el tratamiento se ajuste a la normativa y de responder a las cuestiones y dudas que en esta materia se les susciten a los interesados.

Una de las consultas más frecuentes que se plantean ante el Canal Joven está relacionada con **el tratamiento de datos que realizan empresas de servicios** como, por ejemplo, las de servicios tecnológicos, las encargadas del comedor escolar o de la ruta. En estos casos deben contar con un contrato de encargo de tratamiento con el responsable, por el que el tratamiento de los datos que realizan lo hacen por cuenta y bajo las instrucciones del responsable, sin que ello suponga una comunicación o cesión de datos, es decir, el responsable contrata con una empresa la prestación de un servicio que implica el tratamiento de datos personales personales.

Puede ver más información en el siguiente enlace

QUIÉN ES QUIÉN en el tratamiento de datos personales en tu centro educativo

EL PROFESIONAL RESPONDE

Principios básicos de seguridad: mínimos privilegios y mínima exposición

Seguimos desarrollando en este apartado las mejores técnicas y herramientas para la prevención de los ciberataques.

Existen dos principios básicos de seguridad que hemos de seguir para estar protegidos frente a los múltiples ataques de los que podemos ser víctimas. Son los siguientes:

1º Mínimos privilegios: lo que se pretende es evitar que los usuarios tengan más privilegios de los que necesitan. De esta forma se evitaría que se tenga acceso a servicios e información que solo podrá ser conocida por los administradores. Cuando se usan cuentas de usuario con permisos limitados, se lo ponemos más difícil al atacante para que llegue a datos críticos.

Habría que eliminar las cuentas de usuario que no sean necesarias y las que pertenezcan a empleados que ya no pertenezcan a la empresa.

2º Mínima exposición: hay que evitar la exposición al exterior de la red interna de la empresa. Es necesario que separemos los servidores accesibles desde el exterior de los servidores privados de la organización. Para ello utilizaremos cortafuegos o *firewall*, que establezca reglas para bloquear o permitir conexiones de entrada o salida de nuestra red. En otros casos, esto no bastaría y sería necesario crear una configuración denominada zona desmilitarizada (DMZ).

IMPORTANTE

Se debe revisar cuando contratamos servicios tecnológicos que en los acuerdos de nivel de servicio se incluyan las medidas de mínima exposición.