

LOPD EN LA EMPRESA

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

LA LOPD EN EL DÍA A DÍA

Cuándo es lícito el tratamiento de datos personales según el RGPD

Las empresas, Administraciones Públicas y cualquier otra entidad a quienes les facilitemos datos de carácter personal, están obligadas a cumplir con unos principios y obligaciones previstos en la Ley Orgánica 15/1999 y su Reglamento de Desarrollo. **A partir del 25 de mayo de 2018, serán de aplicación los principios y obligaciones recogidos por el nuevo Reglamento Europeo de Protección de Datos 2016/679, el cual establece que sólo será lícito el tratamiento de datos personales cuando:**

- El interesado haya prestado su **consentimiento previo y explícito**
- El tratamiento sea **necesario para celebrar un contrato** en el que el interesado es parte
- El tratamiento sea necesario **para cumplir con una obligación** impuesta por la Ley a la empresa Responsable
- El tratamiento sea necesario para **proteger intereses vitales** del interesado
- El tratamiento sea necesario para **cumplir una misión (cometido) en interés general o público**
- El tratamiento sea necesario para la **satisfacción de intereses legítimos** perseguidos por el responsable de un tratamiento o por un tercero.

Contenido

Cuándo es lícito el tratamiento de datos personales según...	1
Sanción por envío de correos comerciales no solicitados	2
Control laboral y derecho a la protección de datos	3
La AEPD publica una guía práctica para difundir el.....	4
Riesgos para los datos personales al utilizar Internet	5



IMPORTANTE

Cada uno de los estados miembros de la UE podrá mantener o introducir disposiciones más específicas para adaptar las normas del nuevo Reglamento a su legislación interna.

SANCIONES DE LA AEPD

Sanción por envío de correos comerciales no solicitados

En el [PS/00558/2015](#) vemos la sanción impuesta por la AEPD a un conocido Centro Comercial **por enviar correos publicitarios a un cliente que no habían sido solicitados.**

En abril de 2015 tiene entrada en la AEPD escrito del denunciante manifestando que **tras intentar solicitar la baja del servicio en repetidas ocasiones, sigue recibiendo publicidad y que la cláusula para darse de baja no funciona.**

Tras solicitar las bajas, el denunciante recibía un correo del Centro Comercial en el que se le indicaba **que no figuraba ningún cliente con su dirección de correo,** solicitándole los datos con los que se registró originariamente en la web.

A la vista de los hechos denunciados, los Servicios de Inspección de la Agencia solicitan información al Centro Comercial y piden al denunciante que reenvíe dos correos electrónicos a éste, para analizar los medios de baja que han sido facilitados.

Al analizarse la cuenta del envío, se comprobó que el denunciante había cambiado el servidor que utilizaba, dando lugar a que el Centro Comercial no pudiera dar de baja **al cliente porque la solicitud contenía un nombre y un sólo apellido, careciendo de datos como la dirección de correo electrónico o dirección postal para ponerse en contacto con él, por lo que no les había sido posible atenderla.** Aun así, la directora de la AEPD acordó iniciar el procedimiento sancionador contra el Centro Comercial.

Resultado: multa de 3.300 € a CARREFOUR por una infracción del artículo 21 de la LSSI, tipificada como leve en el artículo 38.4.d) de la misma.

El prestador de servicios deberá ofrecer al destinatario la posibilidad de oponerse al envío en cada mensaje remitido



IMPORTANTE

El tratamiento de datos sin consentimiento, o sin otra habilitación amparada en la Ley, constituye una infracción grave de la LOPD.

LA AEPD ACLARA

Control laboral y derecho a la protección de datos



En el Informe [0464/2013](#) de la AEPD se plantea si es conforme a la Ley Orgánica 15/1999, la entrega a los trabajadores de una empresa, de un Anexo al contrato de trabajo **informando del deber de secreto y confidencialidad, así como del control del uso de Internet y del correo electrónico** de empresa por parte del empleador

–Respecto al **deber de confidencialidad y secreto**, esta obligación viene establecida en la propia LOPD para todas aquellas personas que intervengan en cualquier fase del tratamiento. Es la empresa Responsable quien está obligada a informar a sus trabajadores sobre este deber. Así pues, **el Anexo al contrato cumple con el deber del responsable de adoptar las medidas necesarias para que el personal con acceso a datos personales conozca su deber de secreto.**

–Junto con el deber de confidencialidad, el Anexo informa también sobre **el control por parte del empleador del uso de Internet y del correo electrónico de empresa por los trabajadores**, facultad prevista en el Estatuto de los Trabajadores frente al derecho a la protección de datos de los trabajadores.

La Sentencia del Tribunal Supremo de 26 de septiembre de 2007, concluye que *“la utilización de medios que sean propiedad de la empresa y que ésta facilita al trabajador para cumplir la prestación laboral, está dentro del ámbito del poder de vigilancia del empresario debiendo informarse a los trabajadores de que se va realizar dicho control, así como de los medios que van a aplicarse”*.

Por tanto, puede hacerlo, pues **mediante la firma del Anexo al contrato de trabajo, la empresa estaría informando al trabajador para que el acceso a los equipos informáticos de los empleados sea lícito por su parte.**



IMPORTANTE

La firma del interesado en un documento es el medio más eficaz con el que el empresario puede probar que informó a sus trabajadores.



ACTUALIDAD LOPD

La AEPD publica una guía práctica para difundir el derecho a la protección de datos entre los ciudadanos

Fuente: www.agpd.es

La AEPD publica una guía práctica para difundir el derecho a la protección de datos entre los ciudadanos

'Protección de Datos: Guía para el Ciudadano' recoge numerosas referencias a los cambios que incorpora el nuevo Reglamento General, que será aplicable el 25 de mayo de 2018, e incluye las principales novedades respecto al ejercicio de derechos.

- Repasa los tradicionales derechos ARCO e incluye otros como el derecho al olvido, el nuevo derecho a la portabilidad, o la forma de solicitar la eliminación de fotos y vídeos en internet y qué hacer en caso de no recibir respuesta
- Contiene ejemplos de los tratamientos de datos que más afectan a los ciudadanos, como ocurre en el caso de las comunidades de vecinos, los llamados ficheros de morosos, la videovigilancia o la publicidad, entre otros

(Madrid, 25 de mayo de 2017). La Agencia Española de Protección de Datos (AEPD) ha presentado '[Protección de Datos: Guía para el Ciudadano](#)' en el marco de la 9ª Sesión Anual de la AEPD, un documento que recoge de forma práctica las claves necesarias para que los ciudadanos conozcan qué derechos les amparan y cómo ejercerlos, y qué obligaciones deben cumplir aquellos que traten sus datos personales. Los datos que maneja la Agencia respecto a las consultas recibidas constatan la importancia que los ciudadanos conceden a la protección de sus datos personales y a su privacidad. Así, en 2016 la AEPD recibió cerca de 237.000 consultas, casi un 9% más que en 2015. Por su parte, el Barómetro del CIS de febrero de 2017 también destacó esa importancia al señalar que al 76% de los españoles les preocupa la protección de datos personales y el posible uso de su información personal por terceros.

El Reglamento General de Protección de Datos (RGPD), que comenzará a aplicarse el 25 de mayo de 2018, implica cambios respecto a la normativa actual. Por ello, la Guía para el ciudadano contiene numerosas referencias a la nueva normativa, incluyendo las principales novedades respecto al ejercicio de derechos, detallando qué se puede solicitar en cada uno de los casos.

La Guía repasa los tradicionales derechos de acceso, rectificación, cancelación y oposición (derechos ARCO), la forma de ejercerlos y los plazos legales en los que el ciudadano debe obtenerse una respuesta, incluyendo también aspectos relacionados con el nuevo derecho a la portabilidad, en qué consiste y cómo ejercer el derecho al olvido, o cómo solicitar la eliminación de fotos y vídeos de internet.

Asimismo, la Guía contiene ejemplos de los tratamientos de datos que más repercusión pueden tener en los ciudadanos, como ocurre con los llamados ficheros de morosos, describiendo los requisitos que deben cumplirse para que los datos de una persona puedan ser incluidos en uno de estos ficheros. En este sentido, la inclusión indebida en ficheros de morosidad produce unos efectos especialmente negativos para los afectados, por lo que es imprescindible que las empresas extremen su diligencia antes de comunicar una información inexacta. Por otro lado, el documento recoge otros ámbitos concretos en los que se efectúan tratamientos de datos, como las comunidades de vecinos, la videovigilancia o la publicidad.

Puede ver más información en el siguiente enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_05_25_02-ides-idphp.php

EL PROFESIONAL RESPONDE

Riesgos para los datos personales en el uso de Internet

El incremento de servicios de internet, (correo electrónico, buscadores, Redes Sociales, etc.) han logrado grandes avances en los sistemas de información de un tiempo para acá. Sin embargo **esto conlleva posibles peligros a los que se enfrentan sus usuarios**. Para hacer un uso seguro y responsable, los usuarios:

- Deberán **configurar correctamente la privacidad** de su perfil en las redes sociales
- Deberán **proteger su correo electrónico de ataques de ingeniería social** (virus, gusanos y malware en general).
- Deberán **utilizar el campo "Con Copia Oculta"** cuando se envían mensajes de correo a varios destinatarios
- Deberán utilizar **mecanismos que garanticen la confidencialidad** en el intercambio de información
- Deberán **tener precaución con las conversaciones de los chat**, pues los mensajes circulan por equipos de usuarios desconocidos
- Deberán **facilitar a los buscadores sólo los datos necesarios para la prestación de sus servicios** y no más, pues a través de su análisis, pueden realizarse perfiles de hábitos de navegación
- **No deberán publicar información o imágenes de terceros** sin consentimiento
- **No deberán publicar excesiva información personal**, pues podría identificar y localizar al usuario, incluso de forma física.



IMPORTANTE

Internet ofrece grandes ventajas y herramientas que facilitan el trabajo en gran medida, pero también conlleva enormes peligros que podemos y debemos evitar.