

LOPD

EN LA EMPRESA

LA LOPD EN EL DÍA A DÍA

Cómo notificar ficheros públicos de Ayuntamientos en el RGPD

Según el RDLOPD, todo fichero de datos de carácter personal ya sea de titularidad pública o privada, deberá ser notificado a la AEPD para su inscripción en el RGPD.

Los Ayuntamientos, como entes públicos que tratan datos personales, **deberán hacer lo propio** para adecuarse a la LOPD.

La notificación, modificación o supresión se diferencia de la de los ficheros privados:

- Deberá aprobarse por acuerdo de sus órganos de Gobierno, a través de una norma o Disposición General.
- Dicho acuerdo o Disposición deberá **contener**: la identificación del responsable, la finalidad y usos previstos, el origen de los datos, el procedimiento de recogida, la estructura del fichero y los datos a tratar, las cesiones previstas, los servicios o unidades ante los que se pueden ejercitar los derechos ARCO y las medidas de seguridad a aplicar.
- Una vez aprobado en Junta, el acuerdo o Disposición deberá ser publicado íntegramente en el BOP.
- En el plazo de 30 días desde que fuera publicado en el BOP, el responsable o quien actúe en su representación, **deberá notificar el fichero a la AEPD para su inscripción o modificación en el RGPD.**

Contenido

Cómo notificar ficheros públicos de Ayuntamientos en el RGPD	1
Sanción por realizar una venta de cartera de deuda	2
Hasta qué punto puedo facilitar información a la Agencia...	3
La AEPD e INCIBE presentan la "Guía de privacidad y..."	4
¿Cuándo tengo que firmar un contrato de acceso a datos...	5



IMPORTANTE

La AEPD facilitará modelos o formularios electrónicos a través de su página web para llevar a cabo la creación, modificación o supresión de ficheros de titularidad pública.

SANCIONES DE LA AEPD

Sanción por realizar una venta de cartera de deuda sin informar a los interesados

En el [PS/00650/2014](#) de la AEPD vemos la multa impuesta a un conocido BANCO español por vender una cartera de deuda de sus clientes a otra entidad (PRIME) sin el consentimiento de sus titulares.

En 2013 entra en la Agencia un escrito de, D. A.A.A, declarando haber recibido una notificación de inclusión de sus datos en Asnef por parte de PRIME por una deuda que no reconoce y cuyo pago no le ha sido reclamado previamente.

En investigaciones realizadas por el equipo de inspección de la AEPD se observó que:

- En 2012 el BANCO vendió a PRIME una cartera de deuda entre las que se encontraba una con datos del denunciante.
- En el expediente constan sendas cartas del BANCO y PRIME dirigidas a D. A.A.A. informándole de la compra por PRIME de un crédito adeudado al BANCO.
- En el expediente consta también que la comunicación de cesión de deuda se envió a una dirección en la que el denunciante figuraba como desconocido.
- Del expediente no se acredita que la notificación de la cesión fuera conocida por el denunciante, por lo que dicha comunicación no se produjo, y tal y como establece la LOPD, los datos personales objeto del tratamiento sólo podrán ser comunicados a un tercero con el previo consentimiento del interesado o si está autorizado por ley.

RESULTADO: multa de 6.000 € al BANCO por infracción del artículo 11.1 de la LOPD, tipificada como grave en el artículo 44.3.k) de dicha norma.

Obtener el consentimiento es necesario antes de proceder a la comunicación de datos entre entidades



IMPORTANTE

Las infracciones por cesiones de datos sin el consentimiento de su titular son infracciones graves que conllevan sanciones que van desde 40.001 a 300.000€.

LA AEPD ACLARA

¿Hasta qué punto puedo facilitar información a la Agencia Tributaria?

El Informe [0333/2010](#) de la AEPD se refiere a la **comunicación de datos personales por parte de una entidad a la Administración tributaria a requerimiento de ésta**, pues según establece la LOPD, la comunicación o cesión de datos a un tercero sólo será posible con el consentimiento del interesado, o cuando así esté previsto en una norma con rango de Ley.

La Agencia se ha pronunciado al respecto en diversos informes considerando que dicha **comunicación de datos se encuentra amparada en el artículo 11.2.a) de la Ley Orgánica 15/1999 en conexión con los artículos 93 y siguientes de la Ley General Tributaria**, los cuales imponen una **obligación de información a aquélla**, sobre cualesquiera datos vinculados o que **hagan referencia a las relaciones económicas, profesionales o financieras de las empresas con otras personas**, siempre que dichos datos revistan trascendencia tributaria.

Así pues, las entidades a las que les realice un requerimiento por la Administración tributaria, deberán facilitar la información siempre y cuando se cumplan estos dos requisitos:

- 1- Que los datos estén **vinculados a sus relaciones económicas, profesionales o financieras** con otras personas.
- 2- Que dichos datos **tengan trascendencia tributaria**.

No obstante, será preciso que la cesión de datos **respete el principio de proporcionalidad** del artículo 4.1 de la LOPD, por el que los datos personales sólo se podrán recoger y ser tratados cuando sean **adecuados, pertinentes y no excesivos respecto al ámbito y finalidades determinadas, explícitas y legítimas** para las que se hubieran obtenido.



IMPORTANTE

La comunicación de datos personales entre Administraciones Públicas será posible cuando sea necesaria para el ejercicio de las mismas competencias o que versen sobre las mismas materias.

ACTUALIDAD LOPD



La AEPD e INCIBE presentan la "Guía de privacidad y seguridad en internet"

Fuente: www.agpd.es

La AEPD e INCIBE presentan la 'Guía de privacidad y seguridad en internet', con consejos y recomendaciones prácticas para el ciudadano

La publicación, que incluye 18 fichas que analizan y ofrecen soluciones a los problemas más comunes que pueden surgir en un mundo hiperconectado, se complementa con seis vídeos tutoriales en los que se muestra cómo acceder a las configuraciones de privacidad y seguridad de algunos de los servicios más populares de internet.

(Madrid, 7 de octubre de 2016). La Agencia Española de Protección de Datos (AEPD) y el Instituto Nacional de Ciberseguridad (INCIBE), entidad dependiente del Ministerio de Industria, Energía y Turismo, han presentado hoy en la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI) la '[Guía sobre Privacidad y seguridad en internet](#)'.

Esta iniciativa es el resultado de una apuesta conjunta de ambos organismos para concienciar a los usuarios de la importancia de proteger su información personal, ofreciendo consejos y recomendaciones prácticas. El proyecto cuenta con la colaboración de la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN) del Ministerio de Sanidad, Servicios Sociales e Igualdad; Policía; Guardia Civil; y Telefónica.

El evento ha sido inaugurado por la directora de la AEPD, Mar España, que ha destacado la importancia ofrecer herramientas prácticas para fomentar e impulsar la **cultura de protección de datos** entre los ciudadanos, y el director general del INCIBE, Miguel Rego, que ha insistido en la necesidad de que los ciudadanos adopten una **actitud proactiva** en cuanto al hábito de actualizar y ampliar sus conocimientos sobre seguridad, como medida preventiva para usar las nuevas tecnologías con confianza.

Buena parte de los servicios más populares de la Red se prestan utilizando gran cantidad de información y datos personales que aportan los propios usuarios. La Agencia e INCIBE consideran que la privacidad y la seguridad son aspectos fundamentales que deben tenerse en cuenta para minimizar los riesgos que pueden llegar a producirse en un mundo hiperconectado.

El objetivo de la 'Guía sobre Privacidad y seguridad en Internet' es ofrecer información práctica sobre cómo reducir esos riesgos a los que pueden exponerse cuando utilizan determinados servicios. Con un total de 18 fichas prácticas, en ellas se abordan temas como la importancia de proteger los dispositivos portátiles; generar y gestionar contraseñas; en qué consiste la verificación en dos pasos; cómo realizar copias de seguridad o proteger el correo electrónico; configurar el navegador para que no almacene todos los pasos que se dan mientras se navega por internet; gestionar la información que se almacena en la nube; configurar el perfil en las redes sociales o dónde recurrir para educar a los menores en un uso seguro de internet, sin olvidar temas como el *phishing* o la protección de redes WIFI.

Puede ver más información en el siguiente enlace:

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/nws/2016_10_07-ides-idphp.php

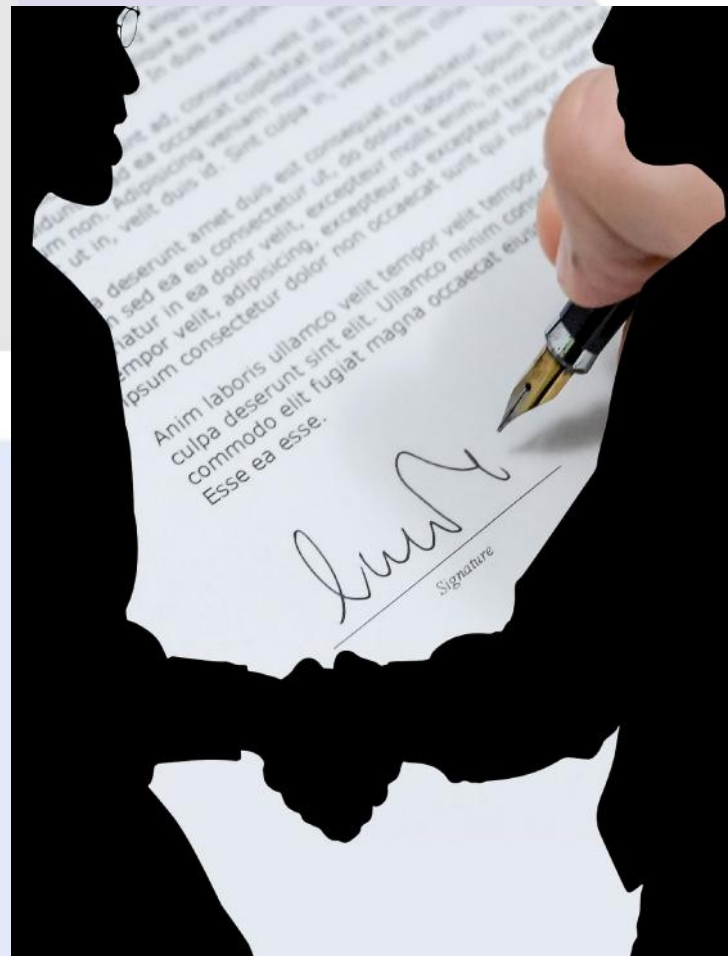
EL PROFESIONAL RESPONDE

¿Cuándo tengo que firmar un contrato de acceso a datos por cuenta de terceros?

Debemos hacer un contrato de acceso a datos por cuenta de terceros con los encargados del tratamiento, es decir, con todas las **empresas externas que accedan, puedan acceder o a las que suministremos datos personales** con la finalidad de prestarnos un servicio.

Estos son algunos de los encargados del tratamiento que pueden existir:

- Consultora de la LOPD.
- Mantenimiento informático de hardware y/o videovigilancia.
- Proveedor/soporte de software.
- Servicio de prevención de riesgos laborales y de la vigilancia de la salud.
- Asesoría laboral, fiscal y/o contable.
- Consultora de calidad, medioambiente, SGSI, etc.
- Certificadora de la norma de calidad, medioambiente, SGSI, etc.
- Proveedor de alojamiento y/o correo electrónico.
- Diseño web, comercio electrónico, etc.
- Organizadora y/o impartidora de formación para los trabajadores.
- Envío de mailings.



IMPORTANTE

Como Responsables de Fichero, deberán firmar el contrato de encargado del tratamiento antes de comenzar la prestación del servicio