Boletín 08/18

LOPD EN LA EMPRESA

Aselio | PROTECCIÓN DE DATOS

AUTOR: JULIO CÉSAR MIGUEL PÉREZ

El EL RGPD UE 2016/679 EN APLICACIÓN

Regulación de transferencias de datos a terceros países (I)

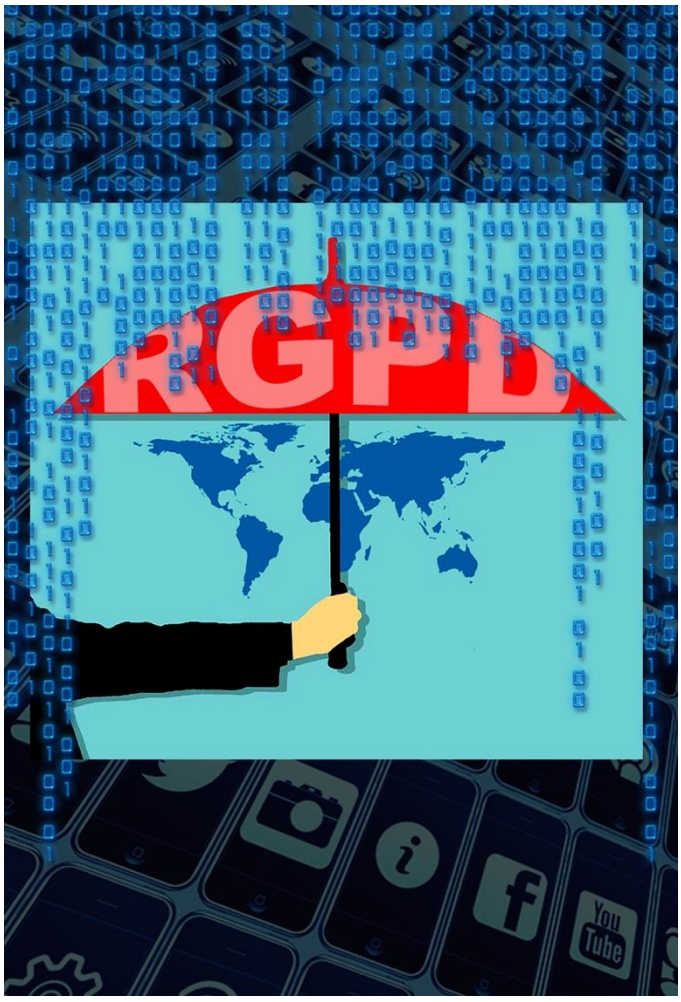
En el mundo globalizado en el que nos encontramos se hacía imprescindible una **regulación común en materia de protección de datos fuera de las fronteras europeas**, y es lo que se ha conseguido con el actual Reglamento Europeo de Protección de datos.

Desde el momento en que comunicamos y enviamos datos personales fuera de la UE, estamos realizando una transferencia de datos a un tercer país (así por ejemplo, si utilizamos un servicio externo de e-mail y éste se encuentra ubicado en EE.UU).

Su regulación, que analizaremos en los siguientes boletines, podemos resumirla en:

- **Transferencias basadas en una decisión de adecuación por la Comisión Europea**. Según ***art.45RGPD***, no será necesaria ninguna autorización previa, siempre que la Comisión considere que ese país u organización internacional cumple con un nivel adecuado de protección.
- **Transferencias mediante las garantías adecuadas**. Todos los supuestos se recogen en el ***art.46.RGPD***
- **Transferencias mediante normas corporativas vinculantes**, regulado en el ***art.47RGPD***.

Contenido



IMPORTANTE

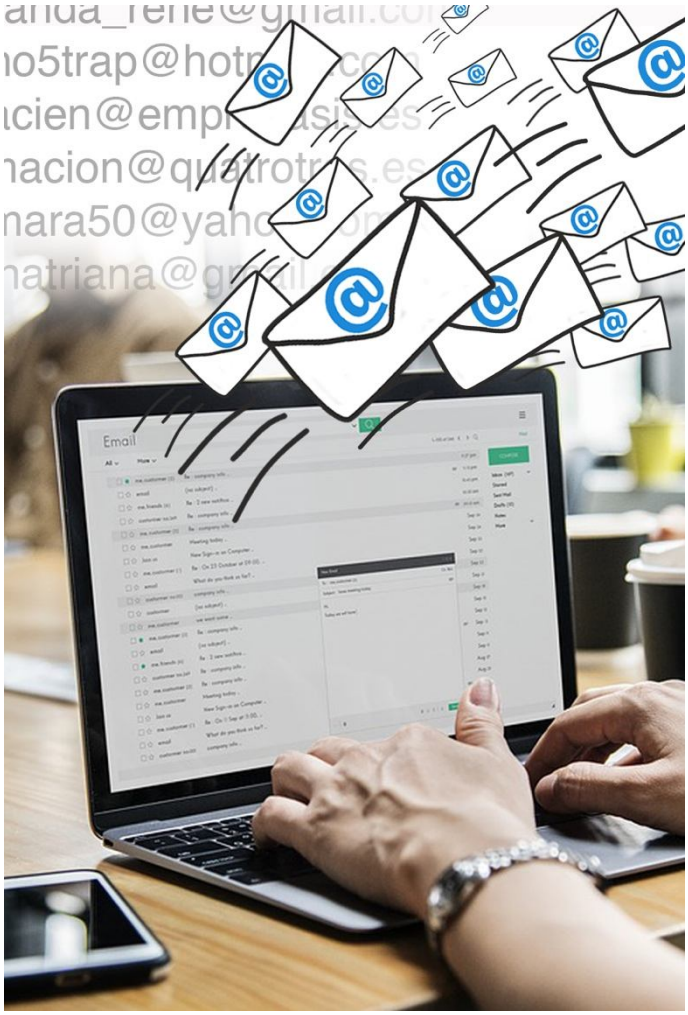
Cuando nos sea imposible garantizar de otro modo, la transferencia de datos a un tercer país, aplicaremos las excepciones para situaciones específicas del ***art.49RGPD***

SANCIONES DE LA AEPD

Apercibimiento por comunicación de correos electrónicos de otros titulares

> ***Art.18 CE.*** *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

En el procedimiento A/00244/2018, instruido por la Agencia Española de Protección de Datos a la entidad **IMPRONTA SOLUCIONES S.L.** vista la denuncia presentada por D.AAA, manifestando que había recibido el 5/03/2018 un **correo electrónico dirigido a múltiples destinatarios con todas las direcciones visibles.**



La Directora de la Agencia decidió someter a **trámite de audiencia previa el procedimiento de apercibimiento**, en virtud del ***art.45.6 de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal***, en adelante (LOPD) en relación a la denuncia por infracción tipificada como grave según el ***art. 44.3.d***, del ***art.10 LOPD***, ***incumplimiento del Deber de guardar secreto profesional*** a cerca del tratamiento de los datos personales por parte de la entidad IMPRONTA SOLUCIONES S.L., obligación que **subsiste con carácter indefinido hacia el afectado**, aún después de finalizar sus relaciones con el titular del fichero o en su caso con el responsable del mismo.

Del escrito de alegaciones presentado por el denunciado, la **Directora de la Agencia acuerda el archivo de las actuaciones**, estimando que **la denunciada estableció, inmediatamente después de conocer el hecho, medidas correctoras** tales como impartición de formación sobre deber de secreto y confidencialidad y otras herramientas técnicas para impedir este tipo de actuaciones en el futuro.

IMPORTANTE

Según la Audiencia Nacional, el deber de sigilo resulta imprescindible en las sociedades actuales, en las que la técnica sitúa a las personas en zonas de riesgo, para la protección de sus derechos fundamentales.

LA AEPD ACLARA

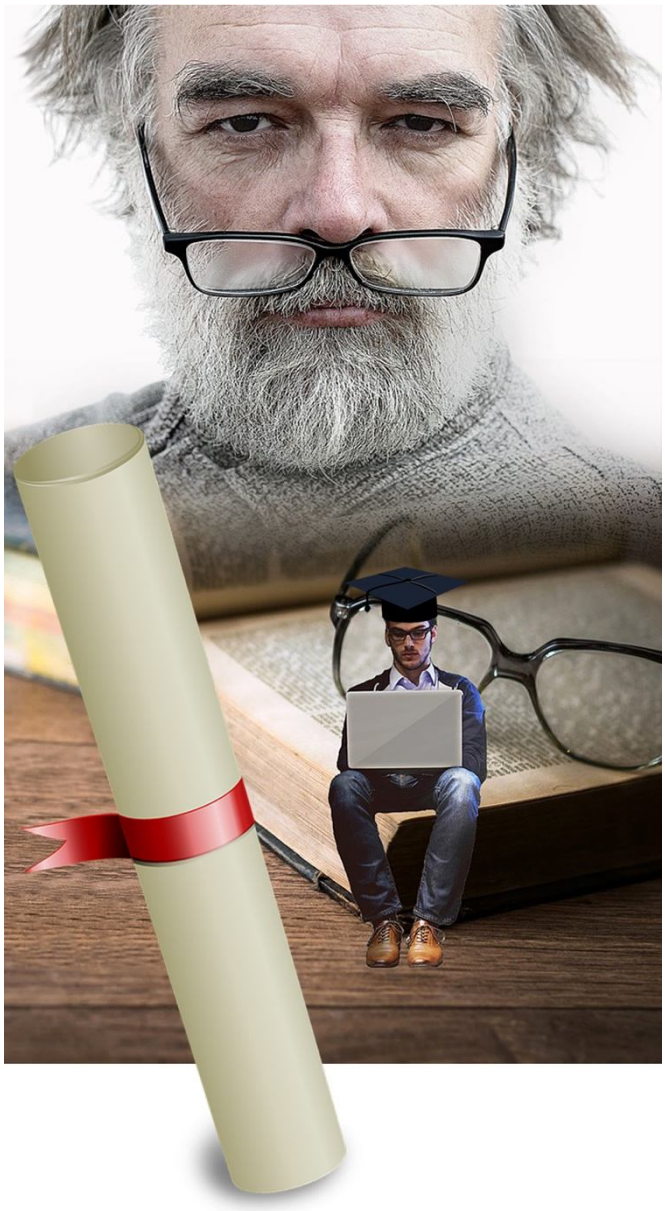
Comunicar datos académicos de los universitarios a sus progenitores

El informe resuelve si es conforme a la normativa de protección de datos la comunicación de datos académicos de los alumnos, de la universidad consultante, a sus progenitores.

A los efectos del art. 4.1 del Reglamento (UE)2016/679 se entiende como dato personal, toda información sobre una persona física identificada o identificable, directa o indirectamente, mediante un identificador, como por ejemplo un nombre, un número de identificación(...) por lo que los datos relativos a matrículas, calificaciones o becas son datos personales protegidos por el Reglamento (UE) 2016/679.

Dicha comunicación constituye un tratamiento de datos, el cuál debe encontrarse fundado en alguna de las causas legitimadoras del art.6 de citado reglamento, y que, en el caso que nos ocupa sería el interés legítimo del responsable.

El pretendido cesionario alega la necesidad de la comunicación de los datos, para aportar como prueba en un procedimiento judicial, con la finalidad de modificar la pensión alimenticia.
Estamos ante una ponderación de dos derechos fundamentales, el derecho a la tutela judicial efectiva de los progenitores y el derecho a la protección de datos personales del alumno, plasmado en multitud de ocasiones en la jurisprudencia.
En el supuesto planteado, se dan los elementos que permiten dicha comunicación para satisfacer ese interés legítimo fundado en la tutela judicial efectiva.



IMPORTANTE

No obstante, el alumno/a podrá ejercer su derecho de oposición a la comunicación, pudiendo quebrar así la presunción de la existencia de un interés legítimo.

LA AEPD ACLARA

La AEPD publica una guía para protección de datos y prevención de delitos

Fuente: AEPD

Presentación de la Guía

¿Por qué estas orientaciones?

La evolución de las tecnologías de la información y la comunicación y la extensión de su uso a través de los servicios y aplicaciones de Internet, como redes sociales, mensajería instantánea o correo electrónico en dispositivos inteligentes, ha llevado a que se utilicen no sólo como un cauce habitual de comisión de infracciones en materia de protección de datos, sino también para cometer hechos tipificados como delitos. Expresiones como ciberacoso, ciberbullying, sexting, grooming, phising, pharming o carding, que nos van resultando cada vez más familiares, son términos en inglés que identifican situaciones de acoso, amenazas, coacciones, revelación de secretos, delitos sexuales, violencia de género o estafas.

El uso de información (datos) de carácter personal, junto al de las tecnologías de la información y comunicación como las que se desarrollan en Internet, puede dar lugar a la comisión de diversos delitos sin que en ocasiones se llegue a ser consciente de ello.

Muchas de estas conductas delictivas tienen en la utilización de información personal, sin cumplir la normativa de protección de datos, uno de sus elementos sin el cual no se hubieran producido, por ejemplo, accediendo sin autorización a datos protegidos, o cuando se utilizan o modifican datos de carácter personal que pueden perjudicar a otra persona sin su consentimiento.

El uso intensivo que se hace de Internet ha hecho que proliferen este tipo de conductas, por lo que la Agencia Española de Protección de Datos considera útil y oportuno facilitar información sobre sus consecuencias y proporcionar pautas básicas para evitar ser víctimas o incluso cometerlas sin ser consciente de su transcendencia.

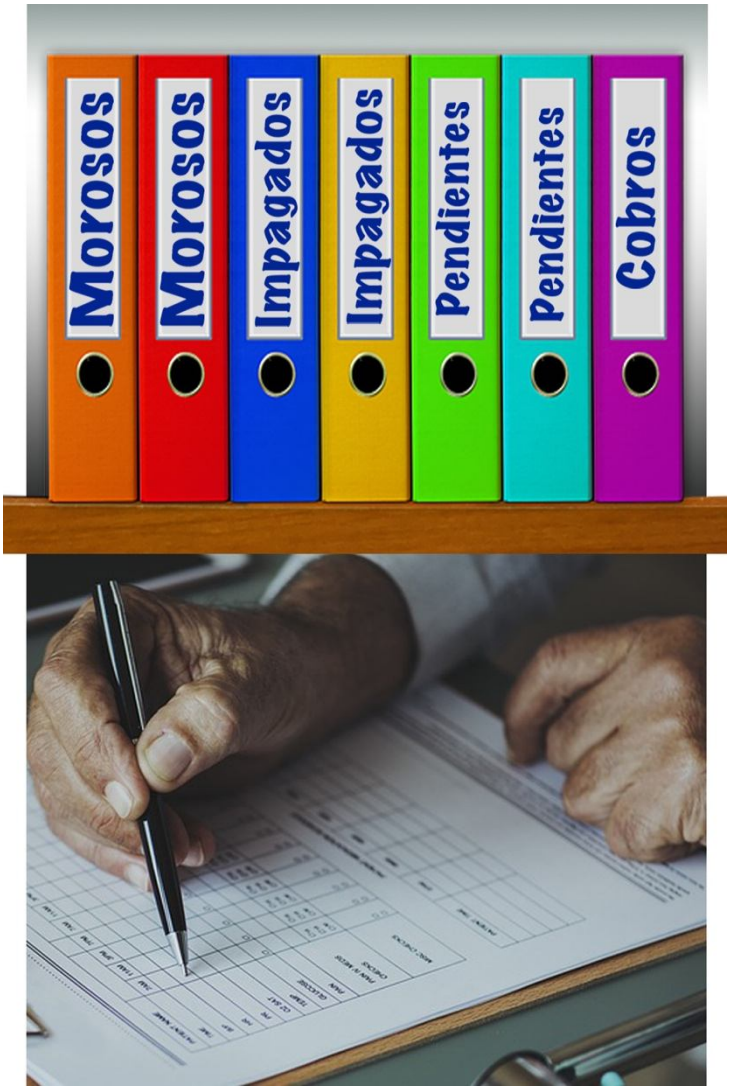
Puede ver más información en el siguiente enlace:

Guía sobre el uso de videocámaras para seguridad y otras finalidades.

LA AEPD ACLARA

Pasos a seguir si tengo que incluir a una persona física en un fichero de Solvencia Patrimonial

Si tuviéramos que incluir a una persona física en un fichero de Solvencia Patrimonial, conocido como “fichero de morosos”, siguiendo lo dispuesto en el ***Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal de 24 de noviembre de 2017***, los pasos a seguir son:



- Lo primero que tenemos que hacer es ser capaces de **probar que se trata de una deuda cierta, vencida, exigible** y que su cuantía no la hayamos reclamado administrativa o judicialmente o por cualquier otro medio alternativo de resolución o bien que no hayan transcurrido seis años desde su obligación.
- En segundo lugar tenemos que haber **informado al afectado de esta posible inclusión en los sistemas de información crediticia, bien en el momento de la celebración del contrato o cuando se vaya a requerir el pago**. En concreto le tendremos que indicar el nombre de los sistemas en los que puede ser incluido. Por su parte, **el responsable de los sistemas debe notificar al afectado** su inclusión en un plazo máximo de 30 días a la notificación de la deuda, durante este periodo los datos permanecerán bloqueados.

Mantendremos los datos durante cinco años, desde la fecha de vencimiento de la deuda, siempre y cuando no haya sido satisfecha antes.

IMPORTANTE

En el momento en que se satisfaga la deuda, el responsable tendrá que comunicarlo al sistema de información crediticia en el plazo de una semana y proceder éste a su supresión.