# NEWSLETTER DE IP-IT – Octubre 2016

**CONTENIDOS**



## 1. *EU-US Privacy Shield*: nuevo marco para la transferencia de datos a EE.UU.

El pasado 12 de julio se aprobó la Decisión de adecuación del Escudo de Privacidad para la transferencia de datos personales desde la Unión Europea a Estados Unidos (en adelante "***EU – US Privacy Shield***" por su denominación en inglés). Tal y como se indicaba en el comunicado emitido por la Comisión Europea, desde el 1 de agosto de 2016, las empresas destinatarias de datos de carácter personal situadas en Estados Unidos, tienen la posibilidad de obtener una certificación ante el Departamento de Comercio de Estados Unidos que les acredite como empresas que disponen de un nivel de protección equiparable al de la normativa europea de protección de datos de carácter personal.

Es importante recordar que, desde que la sentencia de 6 de octubre de 2015 del Tribunal de Justicia de la Unión Europea declarara inválida la Decisión 2000/520/CE, de 26 de julio del 2000, no era posible realizar transferencias de datos a Estados Unidos con base en los principios de puerto seguro publicados por el Departamento de Comercio de Estados Unidos el 21 de julio de 2000 (en adelante el "**Acuerdo de Puerto Seguro**"). De esta manera, el *EU – US Privacy Shield* viene a sustituir dicho Acuerdo de Puerto Seguro, tratando de establecer una equiparación de las legislaciones europea y estadounidense.

De manera similar al sistema que se contenía en el Acuerdo de Puerto Seguro, en el *EU-US Privacy Shield* se incluye un sistema de autocertificación que establece una serie de principios que deben ser cumplidos por las empresas situadas en Estados Unidos que quieran adherirse. Dichos principios son: el principio de notificación, de integridad y limitación de la finalidad, de elección, de seguridad, de acceso, de responsabilidad para la aplicación y recurso (*recourse, enforcement and liability*), y el principio de responsabilidad proactiva para posteriores transferencias (*accountability for onward transfer*). Estos principios, a juicio de la Comisión Europea, suponen para las empresas situadas en Estados Unidos que tratan datos de carácter personal transferidos por una empresa europea, la necesidad de cumplir con obligaciones rigurosas en esta materia; una mayor transparencia en relación con el acceso por la administración estadounidense a los datos personales, así como una protección más eficaz de los derechos de los afectados titulares de los datos de carácter personal.

De conformidad con lo anterior, con el *EU – US Privacy Shield* se endurecen las condiciones para realizar transferencias ulteriores de datos de carácter personal a terceros, ya que la empresa certificada deberá incluir

en los contratos que suscriba con terceros que los datos personales transferidos únicamente podrán ser tratados para aquellas finalidades para las que los titulares otorgaron su consentimiento en el momento de la obtención de los mismos. Adicionalmente, se establece que cualquier ciudadano que considere que sus datos se han utilizado de forma indebida por alguna de las empresas que dispongan de dichos datos, podrá acudir a mecanismos de resolución de litigios gratuitos así como a las autoridades de protección de datos de su correspondiente país, que colaborarán de manera conjunta con la Comisión Federal de Comercio para tratar de que las reclamaciones interpuestas por ciudadanos de la Unión Europea sean investigadas y resueltas.

Asimismo, se llevará a cabo una revisión anual del *EU – US Privacy Shield* por parte de la Comisión Europea y el Departamento de Comercio de los EE.UU. contando con la colaboración de expertos de inteligencia de los Estados Unidos y las autoridades de protección de datos europeas. A este respecto, debe tenerse en cuenta que, tal y como señala el Grupo del artículo 29, la primera revisión anual que se realice del *EU-US Privacy Shield* será clave para poder llevar a cabo una valoración en profundidad de la solidez y eficacia de este nuevo mecanismo.

La empresa que quiera adherirse deberá proporcionar al Departamento de Comercio de Estados Unidos toda la información y documentación acreditativa del cumplimiento de los principios requeridos. El certificado deberá ser renovado por las empresas anualmente, no obstante, el Departamento de Comercio de los Estados Unidos podrá llevar a cabo revisiones periódicas de las empresas adheridas. El listado de empresas que ya se han adherido al *EU-US Privacy Shield* puede consultarse en el siguiente enlace.

• • •

## 2. Tratamiento de datos en los sistemas de denuncia interna (*Whistleblowing*)

El Supervisor Europeo de Protección de Datos ha publicado una guía práctica con recomendaciones sobre el tratamiento de datos de carácter personal en el marco de los sistemas internos de denuncia (*Whistleblowing*), incluyendo una lista de recomendaciones.

En esta guía, el Supervisor hace hincapié en que el sistema de denuncia establezca unos parámetros claros sobre las conductas que pueden notificarse a través del mismo, y sobre el procedimiento a seguir para la investigación posterior que deba realizarse, recalcando la necesidad de respetar el principio de proporcionalidad, no solo en la información recabada, sino también en lo relativo a los periodos de conservación.

Asimismo, destaca la importancia del tratamiento confidencial de la información obtenida a través de estos sistemas de denuncia, aceptando incluso ciertas restricciones al ejercicio de los derechos de información, acceso y rectificación, cuando ello pueda poner en riesgo la investigación que se esté llevando a cabo.

A pesar de que el documento está dirigido a las instituciones y organismos de la Unión Europea que decidan implementar un sistema de denuncia, las recomendaciones y buenas prácticas que detalla pueden extrapolarse a empresas o grupos de empresas que dispongan de este tipo de mecanismos.

• • •

## 3. Responsabilidad de los prestadores de servicios de la Sociedad de la Información por la inclusión de links en páginas web a contenidos protegidos (Sentencia del TJUE de 8 de septiembre de 2016)

El Tribunal de Justicia de la Unión Europea (TJUE) ha publicado una sentencia en la que concluye que la inserción de links que redirigen al usuario a contenidos protegidos constituye una infracción si el prestador de servicios de la sociedad de la información que incluye estos links tiene conocimiento de las consecuencias de su comportamiento, para dar a acceso a una obra protegida. El TJUE matiza que esta actuación constituye un ilícito en la medida en el prestador de servicios lleva a cabo un acto de "comunicación pública" de la obra a un público nuevo que no habría podido acceder, o habría tenido que emplear mayores esfuerzos para acceder al contenido.

La sentencia está relacionada con una cuestión prejudicial que el Tribunal Supremo de los Países Bajos remitió al TJUE, con base en una denuncia de Sanoma, titular de los derechos de unas fotografías, contra GS Media, por redirigir a los usuarios a una web en la que se encontraban disponibles dichas fotografías.

Así, la Sentencia establece que para determinar si la inclusión de links en páginas webs por parte de prestadores de servicios de la sociedad de la información constituye un ilícito se tendrá en cuenta si el prestador de servicios de la sociedad de la información lo lleva a cabo con ánimo de lucro. Esto es así ya que, conforme se indica en la resolución judicial analizada, cuando el que incluye un link en su página web lo lleva a cabo con ánimo de lucro, cabe esperar que de manera previa a la inserción de dicho *link*, haya comprobado la licitud del contenido al que enlaza. Sin perjuicio de lo anterior, el TJUE ha señalado que, si no existe ánimo de lucro y se desconoce que el contenido enlazado es ilícito, la inserción de *links* en páginas webs seguirá siendo lícita. Más Información en el siguiente enlace.

• • •

## 4. *Best practices for Consumer Wereables & Wellness Apps & Devices*

El *Future of Privacy Forum* ha publicado el documento denominado *"Best Practices for Consumer Wereables & Wellness Apps & Devices"* cuyo objetivo es dar unas pautas a los creadores de aplicaciones y dispositivos para determinar si los datos de carácter personal que tratan a través de las denominadas aplicaciones "de salud" o "bienestar" deben ser considerados datos de salud (especialmente protegidos) o no.

En los últimos años se ha incrementado el número de aplicaciones en el mercado relacionadas con la salud o bienestar de los individuos que, muchas veces por desconocimiento, no cumplen con los requerimientos que les son de aplicación de conformidad con la normativa de protección de datos de carácter personal.

Así, el documento incluye un listado de cuestiones que pueden servir como base para que los desarrolladores se hagan una idea de los requerimientos con los que deben cumplir en función del tipo de datos de carácter personal que se tratan a través de las aplicaciones o dispositivos relacionados con la salud o bienestar de los individuos.

Entre dichas cuestiones se encuentran, entre otras, aquellas relacionadas con el contenido que debe ser incluido en la política de privacidad, la obtención del consentimiento de los usuarios, la seguridad que debe ser implementada en los sistemas en los que se alojen datos de carácter personal o las cesiones a terceros de los datos obtenidos a través de las aplicaciones.

• • •

## 5. Reglamento General de Protección de Datos: periodo de transición

La Agencia Española de Protección de Datos ("AEPD") ha publicado recientemente un documento denominado "*Implicaciones prácticas del Reglamento General de Protección de Datos para entidades en el periodo de transición*" en el que, tras afirmar que la nueva norma comporta una gestión distinta de los tratamientos de datos personales, recomienda a los sujetos obligados que vayan adaptando sus procesos para estar preparados en el momento de su aplicación (25 de mayo de 2018).

Asimismo, con anterioridad, la AEPD publicó el documento "*El Reglamento de protección de datos en 12 preguntas*" a través del cual, bajo un formato muy sencillo, aborda alguna de las cuestiones más relevantes de dicho Reglamento General.

Con relación al primero de los documentos, destacamos el contenido relativo al **Consentimiento** en el que, tras señalar que con la entrada en vigor del texto que nos ocupa los tratamientos de datos basados en el

consentimiento tácito no son admisibles, aconseja se revisen dichos consentimientos así obtenidos para adecuarlos al Reglamento. Es asimismo interesante la recomendación formulada por el supervisor en relación al cumplimiento del deber de **Información** (de mayor contenido en relación a nuestra normativa actual), pues aconseja aprovechar el periodo transitorio para completar el contenido de las cláusulas informativas, por ejemplo, a través de las páginas web de los responsables del tratamiento o haciendo uso de los canales de comunicación habituales que mantengan con sus clientes. Destaca asimismo la recomendación sobre la conveniencia de iniciar procesos de las **Evaluaciones de Impacto** sobre la protección de datos (la AEPD ya publicó en su momento la "Guía para una evaluación de impacto en la protección de datos personales") sin perjuicio de que éste no resulte obligatorio hasta la aplicación del Reglamento General. Finalmente, y sin entrar a mayor detalle sobre aspectos relacionados con las certificaciones, es igualmente relevante el contenido referido a las relaciones entre el Responsable y los **Encargados del Tratamiento** ya que recomienda, por un lado, revisar los actuales contratos existentes con vocación de prolongarse más allá de mayo 2018 y, por otro, empezar a incluir las cláusulas contractuales previstas en el Reglamento General.

Finalmente, a través del segundo documento, la AEPD trata de facilitar la comprensión del alcance y consecuencia de la norma, tratando aspectos como su entrada en vigor; los destinatarios; el ámbito de aplicación territorial; los derechos del ciudadano; el principio de "responsabilidad activa" (*accountability*); el consentimiento o la ventanilla única. Destacamos la mención que realiza al consentimiento del menor, respecto del que indica que el límite continua (y no "continuará") en los 14 años.

• • •

**Si desea más información sobre estos temas o cualquier otro asunto relacionado, puede ponerse en contacto con el equipo de profesionales del área de IP-IT de BROSETA.**

## Contactos del área de IP-IT de BROSETA


**Miguel Geijo**
Socio. Director del Área
mgeijo@broseta.com
Tel.: +34 91 432 31 44

**Carolina Vivó**
Abogada
cvivo@broseta.com
Tel.: +34 91 432 31 44

**Alicia Coloma**
Abogada
acoloma@broseta.com
Tel.: +34 91 432 31 44

**Ángela Martínez**
Abogada
angela.martinez@broseta.com
Tel.: +34 96 392 10 06