DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Cuadernos DivalData

Cuadernos dirigidos a delegados,
responsables y especialistas en protección
de datos personales

Cuaderno nº 8 | Febrero 2021

TRANSFERENCIAS INTERNACIONALES DE DATOS. PRINCIPALES CONSECUENCIAS TRAS LA ANULACIÓN DEL PRIVACY SHIELD

Í N D I C E

TRANSFERENCIAS INTERNACIONALES DE DATOS. PRINCIPALES CONSECUENCIAS TRAS LA ANULACIÓN DEL PRIVACY SHIELD

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdssi@dival.es

SUSCRIPCIONES

Si deseas suscribirte a nuestra publicación accede al siguiente

enlace

"TRAS LA ANULACIÓN DEL PRIVACY SHIELD, TODAS AQUELLAS TRANSFERENCIAS DE DATOS AMPARADAS EN EL MISMO, DEJAN DE OFRECER GARANTÍAS Y, POR TANTO, DEBEN DEJAR DE TRANSFERIRSE DATOS EN BASE A ESTE ESCUDO O, EN SU CASO, DEBEN BUSCARSE OTROS MECANISMOS QUE OFREZCAN UN NIVEL DE GARANTÍA ADECUADO".

INTRODUCCIÓN

En el marco de la normativa de protección de datos, se entiende por «transferencia internacional» el flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo - EEE (los países de la Unión Europea, además de Liechtenstein, Islandia y Noruega).

Para que una transferencia internacional sea válida, se debe dar cumplimiento a alguna de las condiciones establecidas en el Capítulo V del Reglamento General de Protección de Datos (en adelante, RGPD). Entre estas, se incluye la Declaración de nivel de protección adecuado por la Comisión Europea.

En esta situación se encontraban algunas entidades estadounidenses que, en el marco de la 'Decisión de Ejecución (UE) 2016/1250 de la Comisión, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EEUU'. se comprometían a cumplir una serie de principios de protección de la vida privada, establecidos por el Departamento de Comercio de los Estados Unidos, que permitían el flujo de datos personales entre los países del EEE y Estados Unidos (en adelante, EE.UU.).

No obstante, en fecha 16 de julio de 2020, el Tribunal Superior de Justicia de la Unión Europea (en adelante, TSJUE) dictaba Sentencia en el asunto C-311/18 (Schrems contra Facebook Ireland), invalidando la citada Decisión 2016/1250 («Privacy Shield» o «Escudo de Privacidad»). Esta Sentencia tuvo su origen en la reclamación interpuesta por Max Schrems, usuario de Facebook, por la transferencia internacional de datos desde Facebook Ireland a Facebook Inc., en EE.UU. Éste alegó que el Derecho y las prácticas de los EE.UU. no ofrecían suficiente protección frente al acceso, por parte de las autoridades públicas, a los datos transferidos.

La anulación del «Privacy Shield» supuso que todas las transferencias de datos amparadas en el mismo dejaran de ofrecer garantías y, por tanto, la necesidad de dejar de transferir datos personales en base a este Escudo o, en su caso, de buscar otros mecanismos que ofrezcan un nivel de garantía adecuado.

"LAS ORGANIZACIONES DEBEN REVISAR DETALLADAMENTE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS HACIA ESTADOS UNIDOS, FRECUENTEMENTE DERIVADAS DE CONTRATACIÓN ADMINISTRATIVA DE SERVICIOS TECNOLÓGICOS Y EL USO DE APLICATIVOS DE PROVEEDORES ESTADOUNIDENSES."

Esta cuestión reviste especial complejidad desde el punto de vista de la contratación administrativa de servicios tecnológicos y el uso de aplicativos de proveedores estadounidenses de enorme profusión y popularidad, que hasta ahora hacían uso del «Privacy Shield» para legitimar las transferencias de datos de los países del EEE a EE.UU.

MOTIVOS DE LA ANULACIÓN

El TSJUE consideró que los requisitos del Derecho nacional estadounidense y, en particular, algunos programas que permitían a las autoridades públicas de los EE.UU. acceder a los datos personales transferidos desde la UE a los EE.UU. con fines de seguridad nacional, imponían limitaciones a la protección de los datos personales y no ofrecían garantías sustancialmente equivalentes a las exigidas en el Derecho de la Unión.

Además, no se proporcionaba ninguna vía de recurso judicial contra las autoridades de los EE.UU. a los titulares de los datos.

Como consecuencia de tal interferencia con los derechos fundamentales de las personas cuyos datos se transfieren a ese país tercero, el TSJUE declaró inválida la Decisión de adecuación del «Escudo de Privacidad».

CONSECUENCIAS DE LA ANULACIÓN

El TSJUE invalidó el «Privacy Shield» sin mantener sus efectos y sin conceder ningún periodo de gracia, ya que la legislación estadounidense evaluada por el Tribunal no proporciona un nivel de protección sustancialmente equivalente al garantizado en la UE.

Esto obliga a las organizaciones a revisar detalladamente las transferencias internacionales de datos hacia EE.UU., frecuentemente derivadas de la contratación administrativa de servicios tecnológicos y el uso de aplicativos de proveedores estadounidenses.

Para continuar transfiriendo datos personales a los EE.UU., las organizaciones deberán dar cumplimiento a

"LAS CLÁUSULAS CONTRACTUALES TIPO (CCT) MANTIENEN SU VALIDEZ, AUNQUE SUPEDITADAS A LA EVALUACIÓN DEL NIVEL DE PROTECCIÓN EXIGIDO POR LA LEGISLACIÓN DE LA UE EN EL PAÍS TERCERO Y, EN CASO DE QUE ESTE NO FUERA ADECUADO, A LA EVALUACIÓN DE LA NECESIDAD DE ADOPTAR MEDIDAS COMPLEMENTARIAS PARA GARANTIZAR UN NIVEL DE PROTECCIÓN EQUIVALENTE AL ESTABLECIDO EN EL EEE".

alguna de las condiciones del art. 46 o siguientes del RGPD, que examinaremos a continuación.

OTRAS HERRAMIENTAS DE TRANSFERENCIA

A falta de Decisión de adecuación, se pueden efectuar transferencias internacionales de datos a EE.UU. haciendo uso de otras herramientas establecidas en los artículos 46 a 49 del RGPD. ¿Cómo cuáles?

1. CLÁUSULAS CONTRACTUALES TIPO (CCT)

Las Cláusulas Contractuales Tipo (en adelante, CCT), contempladas en el art. 46 RGPD, son aquellas cláusulas estandarizadas que han sido adoptadas por la Comisión Europea o una autoridad de control.

Son una forma de permitir la transferencia de datos entre países de la Unión Europea y un tercer país, ya que suponen el cumplimiento de determinadas garantías en la protección de los datos del interesado.

En la citada Sentencia C-311/18 (Maximillian Schrems contra Facebook Ireland), además de la validez del «Privacy Shield», el TSJUE también examinó la 'Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE', manteniendo su validez, aunque supeditándola a la evaluación del nivel de protección exigido por la legislación de la UE en el país tercero y, en caso de que este no fuera adecuado, a la evaluación de la necesidad de adoptar medidas complementarias para garantizar un nivel de protección equivalente al establecido en el Espacio Económico Europeo (EEE).

Por tanto, la posibilidad de transferir datos personales sobre la base de las CCT dependerá del resultado de dicha evaluación, teniendo en cuenta las circunstancias de cada transferencia y las medidas complementarias que haya podido aplicar la entidad estadounidense en cuestión.

"SI SE LLEGA A LA CONCLUSIÓN DE QUE, TENIENDO EN CUENTA LAS CIRCUNSTANCIAS DE LA TRANSFERENCIA Y LAS POSIBLES MEDIDAS COMPLEMENTARIAS, NO SE OFRECERÍAN GARANTÍAS ADECUADAS, SERÍA NECESARIO SUSPENDER O PONER FIN A LA TRANSFERENCIA DE DATOS PERSONALES".

Las CCT, tras un análisis caso por caso de las circunstancias de la transferencia, junto con las medidas complementarias que, en su caso, fueran necesarias, deberían garantizar que la legislación estadounidense no afecte al nivel de protección adecuado.

Si se llega a la conclusión de que, teniendo en cuenta las circunstancias de la transferencia y las posibles medidas complementarias, no se ofrecerían garantías adecuadas, sería necesario suspender o poner fin a la transferencia de datos personales.

En relación con las medidas adicionales, el Comité Europeo de Protección de Datos (CEPD) ha hecho público un documento de recomendaciones sobre medidas que complementarían las herramientas de transferencia para garantizar el cumplimiento del nivel de protección de datos personales de la UE. Este contiene una lista no exhaustiva de ejemplos de medidas complementarias y algunas de las condiciones que necesitarían para ser eficaces. Por ejemplo:

a) MEDIDAS TÉCNICAS

¿Qué medidas técnicas podría adoptar un proveedor de servicios de hosting estadounidense para almacenar datos personales, por ejemplo, con fines de mantener una copia de seguridad?

1. Fuerte encriptación de los datos antes de su transmisión;
2. El algoritmo de cifrado y su parametrización (por ejemplo, la longitud de la clave, el modo de funcionamiento, si procede) se ajustan al estado de la técnica y pueden considerarse robustos frente al criptoanálisis realizado por las autoridades públicas del país receptor, teniendo en cuenta los recursos y las técnicas (por ejemplo, potencia de computación para ataques de fuerza bruta) disponibles para ellos;
3. La fuerza del cifrado tiene en cuenta el período de tiempo específico durante el cual debe preservarse la confidencialidad de los datos personales codificados;

"LAS MEDIDAS ADICIONALES DEBERÁN DECIDIRSE CASO POR CASO, TENIENDO EN CUENTA TODAS LAS CIRCUNSTANCIAS DE LA TRANSFERENCIA".

4. El algoritmo de encriptación se implementa sin problemas mediante un software de mantenimiento adecuado, cuya conformidad haya sido verificada, por ejemplo, por una certificación;
5. Las claves se gestionan de forma fiable;
6. Las claves se conservan únicamente bajo el control del exportador de datos u otras entidades a las que se haya confiado esta tarea que residen en el EEE o en un tercer país, territorio o uno o más sectores específicos dentro de un tercer país, o en una organización internacional para la que la Comisión ha establecido en de conformidad con el artículo 45 del Reglamento sobre la aplicación de la ley, que se garantiza un nivel de protección adecuado.

   En este caso, el CEPD considera que la encriptación realizada sería una medida complementaria efectiva.

b) MEDIDAS ORGANIZATIVAS

El CEPD recomienda métodos de organización y medidas de minimización de datos. Aunque los requisitos organizativos ya existen en virtud del principio de responsabilidad proactiva, supervisados con auditorías periódicas y aplicando también medidas disciplinarias, podrían ser útiles en un contexto de las transferencias. Asimismo, debe considerarse especialmente la minimización de los datos; por ejemplo, cuando la prestación de un servicio sólo requiera la transferencia de un conjunto limitado de datos, no se debe facilitar la base de datos completa. Pero establece como condición la realización de auditorías periódicas y la aplicación de medidas disciplinarias estrictas para vigilar y hacer cumplir las medidas de minimización de datos en el contexto de las transferencias. Además, también exige para considerar válida esta medida complementaria, que las medidas de minimización de datos vayan acompañadas de medidas técnicas.

De todos modos, debemos tener en cuenta que las medidas adicionales deberán decidirse caso por caso, teniendo en cuenta todas las circunstancias de la transferencia.

"CUANDO LAS TRANSFERENCIAS SE BASEN EN EL CONSENTIMIENTO DEL TITULAR DE LOS DATOS, DEBERÁN SER: EXPLÍCITAS; ESPECÍFICAS PARA LA TRANSFERENCIA O CONJUNTO DE TRANSFERENCIAS DE DATOS CONCRETA; E INFORMADAS.

2. CONSENTIMIENTO

Aún es posible transferir datos a los EE.UU. sobre la base de las excepciones previstas en el artículo 49 del RGPD, siempre que se apliquen las condiciones establecidas en dicho artículo. En particular, debe recordarse que cuando las transferencias se basen en el consentimiento del titular de los datos, deberán ser: explícitas; específicas para la transferencia o conjunto de transferencias de datos concreta (lo que significa que el exportador de los datos debe asegurarse de obtener una autorización específica antes de que se ponga en marcha la transferencia, incluso si esto ocurre después de efectuarse la recogida de los datos); informadas, en particular sobre los posibles riesgos de la transferencia (es decir, que el titular de los datos también debería ser informado de los riesgos específicos derivados del hecho de que sus datos serán transferidos a un país que no ofrece una protección adecuada y que no se aplican garantías adecuadas destinadas a garantizar la protección de los datos).

No obstante, el elevado umbral que establece el RGPD para el uso de esta excepción, combinado con el hecho de que el consentimiento prestado por un interesado puede retirarse en cualquier momento, hacen que el consentimiento no sea una solución viable a largo plazo para las transferencias internacionales de datos.

3. EJECUCIÓN DE UN CONTRATO ENTRE EL TITULAR DE LOS DATOS Y EL RESPONSABLE DEL TRATAMIENTO

En este supuesto, debe tenerse en cuenta que los datos personales sólo podrán transferirse cuando la transferencia sea ocasional. Deberá establecerse caso por caso si las transferencias de datos se determinarían como «ocasionales» o «no ocasionales». En cualquier caso, esta excepción sólo podrá invocarse cuando la transferencia sea objetivamente necesaria para la ejecución del contrato.

"PROVEEDORES DE SERVICIOS TECNOLÓGICOS ESTADOUNIDENSES COMO GOOGLE, MICROSOFT, AMAZON, MAILCHIMP O ZOOM, CUYAS HERRAMIENTAS SON FRECUENTEMENTE UTILIZADAS POR ENTIDADES PÚBLICAS Y PRIVADAS, Y CUYAS TRANSFERENCIAS INTERNACIONALES DE DATOS QUEDABAN LEGITIMADAS HASTA EL MOMENTO POR EL «PRIVACY SHIELD», HAN OPTADO POR ADOPTAR CLÁUSULAS CONTRACTUALES TIPO (CCT) PARA REGULARIZAR LAS TRANSFERENCIAS DE DATOS PERSONALES ENTRE PAÍSES DE LA UE Y LOS EE.UU".

4. RAZONES IMPORTANTES DE INTERÉS PÚBLICO

El CEPD recuerda que el requisito sustancial para la aplicabilidad de esta excepción es la constatación de un interés público importante y no la naturaleza de la organización, y que, aunque esta excepción no se limita a las transferencias de datos que son «ocasionales», esto no significa que las transferencias de datos sobre la base de la excepción por razones importantes de interés público puedan tener lugar a gran escala y de manera sistemática. Por el contrario, debe respetarse el principio general según el cual las excepciones establecidas en el artículo 49 del RGPD no deben convertirse en «norma» en la práctica, sino que deben limitarse a situaciones específicas y cada exportador de datos debe garantizar que la transferencia cumpla la prueba de necesidad estricta.

¿POR QUÉ HERRAMIENTA HAN OPTADO LOS PROVEEDORES DE SERVICIOS TECNOLÓGICOS ESTADOUNIDENSES?

Proveedores de servicios tecnológicos estadounidenses como Google, Microsoft, Amazon, Mailchimp o Zoom, cuyas herramientas son frecuentemente utilizadas por entidades públicas y privadas, y cuyas transferencias internacionales de datos quedaban legitimadas hasta el momento por el «Privacy Shield», han optado por adoptar Cláusulas Contractuales Tipo (CCT) para regularizar las transferencias de datos personales entre países del EEE y los EE.UU. Como hemos señalado, las CCT siguen manteniendo su validez, aunque supeditadas a una evaluación que tenga en cuenta las circunstancias de las transferencias y a la adopción de medidas complementarias que ofrezcan garantías adecuadas.

"SI LA ORGANIZACIÓN A LA QUE PERTENECES TRANSFIERE DATOS PERSONALES FUERA DEL ESPACIO ECONÓMICO EUROPEO (UE, ADEMÁS DE NORUEGA, ISLANDIA Y LIECHTENSTEIN), SE DEBE REVISAR EL GRADO DE CUMPLIMIENTO DE ESTAS A LA NORMATIVA DE PROTECCIÓN DE DATOS."

PRODEDIMIENTO PARA LA REVISIÓN DE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS

Si la organización a la que perteneces transfiere datos personales fuera del Espacio Económico Europeo, se debe revisar el grado de cumplimiento de éstas a la normativa de protección de datos.

¿Qué procedimiento podemos seguir para la revisión?

1. Para **detectar las transferencias internacionales de datos,** puede ser de utilidad el Registro de Actividades de Tratamiento (RAT) de nuestra organización. En éste, deberían constar las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional -art. 30 1.e) RGPD-.
2. Comprueba si el país al que se transfieren los datos, es un **destinatario declarado de nivel adecuado por la Comisión Europea** (art. 45 RGPD). Hasta la fecha, los países y territorios declarados como adecuados son: Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda y Japón. Como indicábamos supra, las entidades estadounidenses certificadas en el marco del Escudo de Privacidad UE-EE.UU. ya no se consideran destinatarias de nivel adecuado.
3. A falta de decisión de adecuación, verifica si cumple con alguna de las **garantías que establece el art. 46 RGPD.** En especial, comprueba la existencia de **Cláusulas Contractuales** Tipo aprobadas por la Comisión. Aunque tras la Sentencia del TSJUE estas Cláusulas mantienen su validez, la supeditan a la evaluación del nivel de protección exigido por la legislación de la UE en el país tercero y, en caso de que éste no fuera suficiente, a la evaluación de la necesidad de adoptar medidas complementarias para garantizar un nivel de protección equivalente al establecido en el Espacio Económico Europeo (EEE). En estos casos, habríamos de revisar o instar al proveedor a que justifique que en el tercer país:

"AUNQUE SE HUBIESEN SUSCRITO CLÁUSULAS CONTRACTUALES TIPO, HABRÍAMOS DE REVISAR O INSTAR AL PROVEEDOR A QUE JUSTIFIQUE QUE EN EL TERCER PAÍS: (I) HAY NORMATIVA DE PROTECCIÓN DE DATOS OFREZCA GARANTÍAS SUSTANCIALMENTE EQUIVALENTES A LAS EXIGIDAS EN EL DERECHO DE LA UNIÓN; (II) HAY UNA AUTORIDAD DONDE LOS INTERESADOS PUEDAN RECLAMAR EN MATERIA DE PROTECCIÓN DE DATOS; (III) LA LEGISLACIÓN NO PERMITE QUE LAS AGENCIAS DE INTELIGENCIA PUEDAN ACCEDER MASIVAMENTE Y SIN CONTROL JUDICIAL A LOS DATOS."

- hay normativa de protección de datos ofrezca garantías sustancialmente equivalentes a las exigidas en el Derecho de la Unión;
- hay una autoridad donde los interesados puedan reclamar en materia de protección de datos;
- la legislación no permite que las agencias de inteligencia puedan acceder masivamente y sin control judicial a los datos.

Si el tercer país no cumple con estos requisitos, habrían de aplicarse o instar al proveedor a incluir medidas adicionales en materia de protección de datos, que deberán decidirse caso por caso, teniendo en cuenta todas las circunstancias de la transferencia de que se trate.

4. A falta de garantías adecuadas, la transferencia únicamente se podría realizar si concurre alguna de las **excepciones** del art. 49 RGPD (consentimiento explícito; ejecución de un contrato entre el interesado y el responsable o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado; celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica; razones importantes de interés público; formulación, ejercicio o la defensa de reclamaciones; proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento; registro público que tenga por objeto facilitar información al público).

   Cuando tampoco sea aplicable ninguna de estas excepciones, sólo se podrá llevar a cabo la transferencia si no es repetitiva, afecta a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evalué todas las circunstancias y, basándose en esta evaluación, ofrezca garantías apropiadas con respecto a la protección de datos personales.

   No obstante, estas excepciones únicamente deben aplicarse con carácter residual, cuando resulte imposible la aplicación de otras herramientas y la transferencia afecte a pocos interesados.

MATERIAL COMPLEMENTARIO

- Información sobre transferencias internacionales (AEPD). Consulta su web en este enlace.
- Sentencia del Tribunal de Justicia de la Unión Europea (TSJUE), de 16 de julio de 2020, asunto C-311/18. Consulta el informe en este enlace.
- Preguntas frecuentes sobre la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311/18 (CEPD). Consulta el documento en este enlace.
- Recomendación 01/2020 sobre medidas que complementan las herramientas de transferencia para garantizar el cumplimiento del nivel de protección de datos personales de la UE (CEPD). Consulta el documento en este enlace.
- Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE. Consulta la Decisión en este enlace.
- Adenda de protección de datos de Microsoft (actualizada a diciembre de 2020). Consulta este enlace.
- Adenda de protección de datos de Google Suite. Consulta este enlace.
- Cláusulas contractuales tipo Google G Suite. Consulta este enlace.
- Instrucciones para aceptar el Contrato de encargo del tratamiento de Google Analytics. Consulta este enlace.
- Instrucciones para aceptar el contrato de encargo del tratamiento y Cláusulas Contractuales Tipo de Google Workspace y Cloud Identity. Consulta este enlace.
- Contrato de protección de datos y Cláusulas contractuales tipo de Mailchimp. Consulta este enlace.

NOTICIAS

- **La Agencia Española de Protección de Datos (AEPD) lanza un Pacto Digital para la protección de las personas que promueve un gran acuerdo por la convivencia ciudadana y fomenta el compromiso con la privacidad de las organizaciones.**

  La iniciativa, a la que ya se han adherido 40 organizaciones empresariales, fundaciones, asociaciones de medios y grupos audiovisuales, supone un compromiso con la privacidad en las políticas de sostenibilidad y los modelos de negocio de empresas y organizaciones. El Pacto se compone de varios documentos: la carta de adhesión, el compromiso por la responsabilidad en el ámbito digital y un decálogo de buenas prácticas para medios de comunicación y organizaciones con canales de difusión propios.

  Consulta la información relativa al Pacto Digital en este enlace.

- **El Comité Europeo de Protección de Datos (CEPD) publica un documento de Directrices 01/2021, sobre ejemplos relacionados con la notificación de violaciones de seguridad.**

  Las Directrices, basadas en casos prácticos, complementan las Directrices WP 250 del GT29 y reflejan la experiencia de las autoridades de control en esta materia desde la entrada en vigor el RGPD. Su objetivo es ayudar a los responsables del tratamiento de datos a manejar las violaciones de seguridad y qué factores tener en cuenta durante la evaluación de riesgos, arrojando luz sobre si se debe notificar o no a la autoridad de control a los interesados. El documento está abierto a consulta pública hasta el 2 de marzo.

  Consulta el documento (únicamente en inglés) en este enlace.