



C/M/S/

Law . Tax

# Guía sobre transferencias internacionales de datos

A partir del caso *Schrems II*

CMS España

Julio 2020



# Guía sobre transferencias internacionales de datos – A partir del caso *Schrems II*

*Javier Torre de Silva, José Luis Piñar y Miguel Recio*

El 16 de julio de 2020, casi cinco años después de la anulación del Acuerdo de Puerto Seguro (“Safe Harbor Agreement”) entre la Unión Europea y los Estados Unidos, la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) dictada en el asunto C-311/18 (caso *Schrems II*) ha invalidado también el Escudo de Privacidad (“Privacy Shield”) entre aquéllos, adoptado para reemplazar al anterior.

Además, el TJUE ha concluido que la Decisión 2010/87/UE de la Comisión, de 5 febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento, es válida.

La sentencia, una de las más importantes sobre protección de datos que ha dictado el TJUE en los últimos años, plantea cuestiones relevantes tanto para quienes transfieren datos personales fuera del Espacio Económico Europeo (EEE) como para la economía digital, que requieren de un marco robusto que dé respuesta a las dudas e incertidumbres que se suscitan.

## Índice

1. El nuevo paradigma europeo para las transferencias internacionales de datos
2. Caso *Schrems II*: una decisión invalidada y otra declarada válida (“con reservas”)
3. ¿Por qué invalida el TJUE la Decisión de Ejecución (UE) 2016/1250 de la Comisión?
4. ¿Qué supone la sentencia del TJUE para las transferencias a Estados Unidos?
5. La sentencia del TJUE, ¿implica que desaparezca el Escudo de Privacidad?
6. La conclusión del TJUE en el caso del Escudo de Privacidad, ¿podría ser aplicable a otros terceros países con una decisión de adecuación de la Comisión?
7. ¿Qué implica la sentencia del TJUE para responsables y encargados del tratamiento en el caso de la Decisión 2010/87/UE sobre cláusulas contractuales tipo?
8. ¿Cuáles son los mecanismos alternativos previstos en el RGPD para transferencias internacionales de datos?
9. Referencias

## 1. El nuevo paradigma europeo para las transferencias internacionales de datos

Uno de los pilares en que se asienta el Reglamento Europeo de Protección de Datos (RGPD) es el de garantizar la tutela del derecho a la protección de datos no sólo en la Unión Europea sino más allá de sus fronteras, cuando el tratamiento de datos pueda afectar a quien se encuentre en la Unión. Los flujos transfronterizos de datos personales (cada vez más numerosos) “son necesarios para la expansión del comercio y la cooperación internacionales”, pero esto no debe suponer que las transferencias menoscaben el nivel de protección garantizado por el Reglamento, ni siquiera en las transferencias ulteriores de datos desde el tercer país a otro diferente (art. 44 y considerando 101 RGPD). A tal fin el RGPD contiene un complejo régimen de las transferencias internacionales (arts. 44 a 50)<sup>1</sup> que incluye la regulación de los mecanismos que permiten garantizar que el lugar de destino de los datos que van a transferirse ofrece un nivel de protección adecuado en relación al que garantiza el RGPD. Entre esos mecanismos, y al objeto de permitir la transferencia de datos a Estados Unidos, la Unión Europea adoptó el llamado sistema de Escudo de Privacidad o *Privacy Shield* (que sustituyó al anterior, llamado de “Puerto Seguro”: “Safe Harbor Agreement”), que ahora el Tribunal de Justicia de la Unión Europea (TJUE), con su Sentencia de 16 de julio de 2020 (asunto C-311/18, caso *Schrems II*), acaba de considerar inválido, lo que afecta a miles de empresas que a diario llevan a cabo cientos de miles de transferencias de datos con incidencia en millones de datos personales. Las consecuencias económicas para las empresas son incalculables, por lo que la Comisión Europea, el mismo día en que se hizo pública la Sentencia, señaló que va a trabajar para poder encontrar cuanto antes una solución a la situación generada.

Además, el TJUE concluye que otro de los mecanismos para garantizar las transferencias internacionales, las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países aprobadas en virtud de la Decisión 2010/87/UE de la Comisión, de 5 febrero de 2010, es válida.

Como ha señalado la Agencia Española de Protección de Datos, la sentencia marca “un nuevo punto de inflexión sobre la forma en la que se realizan las transferencias internacionales de datos a EEUU” y requiere “una respuesta armonizada a nivel europeo”, un enfoque común que garantice “una aplicación consistente de la sentencia en todos los países de la UE”<sup>2</sup>. Por su parte el Comité Europeo de Protección de Datos (EDPB) emitió de inmediato un comunicado en el que llamaba la atención acerca de la necesidad de adoptar un nuevo marco de transferencias internacionales totalmente acorde con la normativa europea de protección de datos<sup>3</sup>.

La trascendencia que para las empresas tiene la Sentencia y las relevantes cuestiones que plantea tanto para quienes transfieren datos personales fuera del Espacio Económico Europeo (EEE) como para la economía digital fueron puestos de manifiesto ya por CMS desde el primer momento<sup>4</sup>, requieren de un análisis en profundidad que dé respuesta a las dudas e incertidumbres que se suscitan.

## 2. Caso *Schrems II*: una decisión invalidada y otra declarada válida (“con reservas”)

La sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 16 de julio de 2020, en el asunto C-311/18, es una continuación de la que dio lugar a la invalidación del Acuerdo de Puerto Seguro (“Safe Harbor Agreement”)<sup>5</sup> entre la Unión Europea y los Estados Unidos.

1. Sobre esta cuestión puede verse: Piñar Mañas, José Luis, “Transferencias de datos personales a terceros países u organizaciones internacionales”, en Piñar Mañas, José Luis (Director), Álvarez Caro, María y Recio Gayo, Miguel (Coordinadores), *Reglamento General de Protección de Datos, Hacia un nuevo modelo europeo de protección de datos*, Reus, Madrid, 2016; y Piñar Mañas, José Luis (Director) y Recio Gayo, Miguel (Coordinador), *Memento Protección de Datos*, Francis Lefebvre, Madrid, 2019.

2. Agencia Española de Protección de Datos, “El Tribunal de Justicia de la Unión Europea declara inválido el Escudo de Privacidad para la realización de transferencias internacionales de datos a EEUU. 22 de Julio de 2020”.

3. *Statement on the CJUE Judgment in Case C-311/18. 17 July 2020.*

4. *Schrems strikes again: EU-US Privacy Shield invalid; Standard Contractual Clauses upheld but due diligence required.*

5. Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América. Invalidada por la sentencia del TJUE (Gran Sala), de 6 de octubre de 2015, asunto C-362/14.

Ambas sentencias tienen por objeto responder a cuestiones prejudiciales planteadas en el marco de las reclamaciones presentadas por un usuario de la red social Facebook contra la transferencia de sus datos personales por Facebook Ireland (Unión Europea) hacia Facebook Inc. (Estados Unidos). Las reclamaciones fueron presentadas, en ambos casos, por un residente austriaco ante la autoridad irlandesa de protección de datos.

Ahora bien, se trata de dos decisiones diferentes a efectos de los mecanismos previstos para las transferencias internacionales de datos, ya que mientras que en la primera sentencia se declara la invalidez de la Decisión relativa al Acuerdo de Puerto Seguro prestando especial atención a las limitaciones al ejercicio de las facultades conferidas a las autoridades de protección de datos, en la segunda sentencia, que invalida la Decisión de Ejecución (UE) 2016/1250, de 12 de julio de 2016, sobre el Escudo de Privacidad<sup>6</sup>, el TJUE centra su atención en las obligaciones de autoridades de protección de datos, así como de responsables y encargados del tratamiento, en garantizar un nivel adecuado de protección de datos.

Además de invalidar la referida Decisión de Ejecución, el TJUE se pronuncia también sobre la validez de las cláusulas contractuales tipo aprobadas en virtud de la 2010/87/UE de la Comisión<sup>7</sup>, de 5 de febrero de 2010. Y, si bien concluye que “a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales” esta Decisión es válida, es necesario considerar que en su texto se incluyen obligaciones para responsables (exportadores) y encargados del tratamiento (importadores), que son esenciales para garantizar el nivel adecuado de protección de datos ya mencionado. Por tanto, si no se adoptan las medidas oportunas, a pesar de que las cláusulas tipo son válidas, no serían suficientes para poder llevar a cabo una transferencia internacional de datos por falta de garantías suficientes. Y en este sentido, como se indica en las preguntas frecuentes aprobadas por el Comité Europeo de Protección de Datos el pasado 23 de julio<sup>8</sup>, tanto el exportador como el importador de los datos personales tendrán que verificar, antes de realizar la transferencia internacional, que el nivel adecuado de protección de datos es respetado en el tercer país. Esta verificación implica que deban tenerse en cuenta las circunstancias en las que se llevará a cabo la transferencia internacional, lo que implica que deba realizarse una evaluación exhaustiva en materia de protección de datos.

### 3. ¿Por qué invalida el TJUE la Decisión de Ejecución (UE) 2016/1250 de la Comisión?

La Decisión de Ejecución (UE) 2016/1250 de la Comisión, ha sido invalidada por el TJUE por ser incompatible con el Reglamento General de Protección de Datos (RGPD)<sup>9</sup>, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE).

En concreto, el TJUE indica que la Comisión “no tuvo en cuenta las exigencias resultantes del artículo 45, apartado 1, del RGPD, interpretado a la luz de los artículos 7, 8 y 47 de la Carta” (apartado 198 de la sentencia en el asunto C-311/18), por lo que es incompatible (apartado 199, C-311/18).

Según el TJUE, el requisito que la Comisión no habría considerado en la Decisión de Ejecución (UE) 2016/1250 de la Comisión es que el tercer país, en este caso Estados Unidos, garantizase un nivel de protección adecuado.

El nivel de protección adecuado tiene que interpretarse conforme a los siguientes derechos fundamentales:

— Respeto de la vida privada y familiar (art. 7 de la CDFUE);

---

6. Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU.

7. 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 del Parlamento Europeo y del Consejo.

8. Disponibles en: [https://edpb.europa.eu/news/news/2020/european-data-protection-board-publishes-faq-document-cjeu-judgment-c-31118-schrems\\_en](https://edpb.europa.eu/news/news/2020/european-data-protection-board-publishes-faq-document-cjeu-judgment-c-31118-schrems_en).

9. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

- Protección de datos de carácter personal (art. 8 de la CDFUE), y
- Derecho a la tutela judicial efectiva y a un juez imparcial (art. 47 de la CDFUE).

## 4. ¿Qué supone la sentencia del TJUE para las transferencias a Estados Unidos?

Desde el 16 de julio de 2020 ya no pueden llevarse a cabo transferencias internacionales de datos personales a Estados Unidos sobre la base del Escudo de Privacidad al haber sido invalidado por el TJUE. Al ser Estados Unidos un tercer país que carece de nivel adecuado de protección, de manera que el responsable del tratamiento o el encargado del tratamiento establecidos en la Unión Europea deberán recurrir a alguno de los demás mecanismos previstos en el RGPD para proporcionar garantías adecuadas.

Es decir, el Escudo de Privacidad deja de ser una opción a efectos de poder transferir datos personales desde la Unión Europea a una empresa que esté adherida a aquél. Las transferencias de datos a Estados Unidos tendrán que basarse en otra garantía adecuada, tal como las cláusulas contractuales tipo, cláusulas tipo adoptadas por una autoridad de protección de datos y aprobadas por la Comisión o normas corporativas vinculantes (BCRs).

Si en el futuro se alcanzase otro acuerdo entre la Unión Europea y los Estados Unidos, podrán volver a llevarse a cabo transferencias de datos a empresas adheridas al programa que sustituya al Escudo de Privacidad, lo cual no es descartable dado el interés mostrado a ambos lados del Atlántico.

Desde un punto de vista económico, el Departamento de Comercio ha manifestado que la invalidación del Escudo de Privacidad podría tener un impacto negativo para una relación comercial transatlántica de más de siete (7) trillones de euros, así como que las empresas europeas tendrán que recurrir a otros mecanismos para transferencias internacionales de datos si quieren acceder a los servicios prestados por las más de 5.300 empresas adheridas al Escudo de Privacidad<sup>10</sup>.

## 5. La sentencia del TJUE, ¿implica que desaparezca el Escudo de Privacidad?

Aunque el TJUE haya invalidado la Decisión de Ejecución (UE) 2016/1250 de la Comisión, el Escudo de Privacidad no desaparece para las empresas estadounidenses adheridas o que se adhieran.

Es necesario tener en cuenta que la invalidación implica que los responsables del tratamiento que transfieren datos personales desde el EEE a las empresas adheridas al Escudo de Privacidad no pueden recurrir a este mecanismo, de manera que desde el 16 de julio de 2020 toda transferencia internacional de datos en virtud del Escudo de Privacidad requiere de otras garantías adecuadas para que pueda llevarse a cabo.

No obstante, el Secretario de Comercio de los Estados Unidos, en una declaración sobre la sentencia del TJUE<sup>11</sup>, indicó que el Departamento de Comercio (*Department of Commerce*) seguirá administrando el Escudo de Privacidad, atendiendo las solicitudes de autocertificación y de recertificación, además de mantener el listado de empresas adheridas que puede consultarse [aquí](#).

La administración del programa del Escudo de Privacidad corresponde al Departamento de Comercio, en virtud de lo previsto en el Anexo I de la Decisión de Ejecución (UE) 2016/1250 de la Comisión.

---

10. *U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows*.

11. *Ibid.*

## 6. La conclusión del TJUE en el caso del Escudo de Privacidad, ¿podría ser aplicable a otros terceros países con una decisión de adecuación de la Comisión?

La conclusión alcanzada por el TJUE sobre el Escudo de Privacidad podría darse en el caso de otros países a la vista del requisito de garantizar un nivel de protección adecuado, que será similar o equivalente al de la Unión Europea. Como ya señaló el TJUE en la sentencia de 5 de octubre de 2015 cuando invalidó el Acuerdo de Puerto Seguro, se trata de que el tercer país proporcione “una protección sustancialmente equivalente a la garantizada en la Unión” (apartado 73 de la sentencia en el asunto C-362/14), sin que se trate de “exigir que un tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión”.

El requisito mencionado, que debe interpretarse y aplicarse conforme a los derechos fundamentales previstos en la CDFUE, es aplicable a cualquier tercer país u organización internacional fuera de la Unión Europea, debiendo tener en cuenta al respecto que el RGPD se aplica también en los países del Espacio Económico Europeo.

A diferencia de la decisión de adecuación, es importante señalar que las otras decisiones de la Comisión sobre el nivel adecuado de protección de datos, tales como las relativas a cláusulas contractuales tipo, se refieren a “diversos tipos de sistemas de protección de los datos personales”<sup>12</sup> derivados de diferentes tradiciones jurídicas.

## 7. ¿Qué implica la sentencia del TJUE para responsables y encargados del tratamiento en el caso de la Decisión 2010/87/UE sobre cláusulas contractuales tipo?

A pesar de que el TJUE declara válida la Decisión 2010/87/UE, recuerda y resalta que tanto los responsables y encargados del tratamiento como las autoridades de protección de datos tienen obligaciones en virtud del RGPD por lo que se refiere a garantizar el derecho fundamental a la protección de datos cuando se lleva a cabo una transferencia internacional de datos. En concreto, la sentencia del TJUE subraya que “a falta de una decisión de adecuación, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas” (apartado 128, C-311/18), lo que podría hacerse a través de las cláusulas tipo. Y esto, a diferencia de lo que ocurría hasta la aplicación del RGPD, implica que “pueda ser necesario completar las garantías recogidas en esas cláusulas tipo de protección de datos” (apartado 133, asunto C-311/18).

A modo de primeros pasos, es recomendable que el responsable del tratamiento que va a transferir datos personales desde el EEE sobre la base de las cláusulas contractuales tipo aprobadas en virtud de las cláusulas contractuales tipo, proceda a:

- i. **Comprobar caso por caso, considerando las circunstancias específicas, así como la legislación aplicable en el tercer país**, y, si fuera necesario en colaboración con el destinatario de la transferencia; si dicho país (fuera del EEE) garantiza una protección adecuada, en particular por lo que se refiere al acceso gubernamental a los datos personales, ya sea en tránsito o cuando son tratados en el tercer país;
- ii. Como parte del análisis anterior, el responsable del tratamiento deberá **atender a si se transfieren categorías especiales de datos** y, si fuera así, **informar**:
  - “al interesado antes de que se efectúe la transferencia o en cuanto sea posible” (apartado 144, asunto C-311/18) y

---

12. Comisión Europea (2017). *Comunicación de la Comisión al Parlamento Europeo y al Consejo. Intercambio y protección de datos personales en un mundo globalizado*. COM(2017) 7 final. Bruselas, p. 7.



- de manera que el interesado pueda “ejercer el derecho de recurso contra el responsable del tratamiento” (apartado 144, asunto C-311/18).
- iii. **A notificar a la autoridad de protección de datos una modificación en la legislación que es aplicable al importador en el tercer país que tenga un “importante efecto negativo sobre las garantías ofrecidas y las garantías impuestas por las cláusulas tipo de protección de datos”** (apartado 145, asunto C-311/18), cuando el importador o destinatario de la transferencia se lo notifique;
- iv. Si fuera necesario, **adoptar garantías adicionales a las ofrecidas por las cláusulas tipo de protección de datos** como, por ejemplo, la obligación del encargado del tratamiento de informar y adoptar medidas cuando reciba solicitudes gubernamentales de acceso a los datos personales en el tercer país;
- v. **Analizar o evaluar la efectividad de las garantías adicionales**, ya que será necesario demostrar que, en la práctica, queda garantizada la protección adecuada de los datos;
- vi. **Tener presente su facultad de suspensión o finalización de la transferencia internacional**, lo que podría implicar la rescisión del contrato, al país de destino cuando no exista una protección adecuada y, en su caso, considerar que la autoridad de protección de datos puede ordenar dicha suspensión o terminación;
- vii. También debería tenerse en consideración que **la negativa o falta de asistencia por el importador de los datos puede dar lugar a que no sea un encargado del tratamiento que ofrece “garantías suficientes”**, debiendo adoptar medidas al respecto en virtud de la obligación de responsabilidad proactiva, y
- viii. **Considerar las implicaciones anteriores en el caso de otros mecanismos** para la transferencia internacional de datos, incluidas las normas corporativas vinculantes.

Cabe también esperar que las autoridades de protección de datos ofrezcan orientación en la materia.

Y si ya se estuvieran llevando a cabo transferencias internacionales de datos:

- i. **Revisar cada transferencia internacional de datos** de manera que se compruebe si estaba basada en el Escudo de Privacidad:
  - Si fuera así:
    - **Verificar si existe una alternativa a dicho mecanismo**, ya que en ocasiones los encargados del tratamiento adheridos al Escudo de Privacidad ofrecían al mismo tiempo otras alternativas o puede que el importador la ofrezca para dar solución a la situación creada por la invalidación del Escudo de Privacidad;
    - Si no se da el supuesto anterior, **detener dicha transferencia por falta de garantías adecuadas** para la transferencia internacional de datos, y
    - Vinculado con el punto anterior, **buscar una alternativa al Escudo de Privacidad**, es decir, otro mecanismo que permita ofrecer garantías adecuadas para la transferencia internacional de datos en ausencia de una decisión de adecuación.

En cualquier caso, el Escudo de Privacidad, al ser invalidado, deja de ser aplicable por lo que se refiere a la posibilidad de recurrir al mismo para aportar garantías adecuadas para la transferencia internacional de datos a empresas adheridas al mismo en Estados Unidos.

- Considerar, en particular, que, si la transferencia internacional no ofrece un nivel de protección adecuado, el responsable del tratamiento tendrá que suspender o finalizar dicha transferencia, pudiendo hacerlo también la autoridad de protección de datos.

En cualquier caso, la evaluación o análisis (“assessment”) de la existencia de un nivel adecuado de protección de datos recae también en el responsable del tratamiento que va a actuar como exportador de datos, lo que obviamente tiene un impacto relevante por lo que se refiere a las medidas a adoptar en materia de protección de datos. Y esta evaluación es fundamental para, si fuera necesario, adoptar garantías adicionales que se añadirán a las cláusulas contractuales tipo.

Una de las principales conclusiones es que los responsables o encargados del tratamiento que exporten datos personales fuera del EEE, con independencia de cuál sea el mecanismo al que recurran, tendrán que llevar a cabo una evaluación (“assessment”) de las garantías en materia de protección de datos que requiere de asesoramiento especializado.

## 8. ¿Cuáles son los mecanismos alternativos previstos en el RGPD para transferencias internacionales de datos?

Al margen de las decisiones de adecuación, el RGPD incluyó otros “mecanismos suficientemente flexibles para adaptarse a distintos tipos de situaciones de transferencia”<sup>13</sup>.

En el caso del sector privado, las garantías adecuadas a proporcionan cuando se transfieren datos personales fuera de la Unión Europea, son:

- Normas corporativas vinculantes (art. 46.2.b) del RGPD).
- Cláusulas contractuales tipo o cláusulas tipo de protección de datos adoptadas por una autoridad de protección de datos y aprobadas por la Comisión (art. 46.2.d) del RGPD).
- Códigos de conducta aprobados conforme a lo previsto en el RGPD, junto con compromisos vinculantes y exigibles (art. 46.2.e) del RGPD).
- Mecanismos de certificación aprobados conforme a lo previsto en el RGPD, junto con compromisos vinculantes y exigibles (art. 46.2.f) del RGPD).

Las normas corporativas vinculantes (*Binding Corporate Rules*, BCRs) fueron creadas en el seno del Grupo de Trabajo del Artículo 29, ya que no estaban previstas en la ya derogada Directiva 95/46/CE, y fueron incluidas en el RGPD. Por lo que se refiere a la posibilidad de recurrir a las mismas, implican un proceso de aprobación por la autoridad líder en caso de grupos de empresas en varios Estados miembros de la Unión Europea. No obstante, como ha indicado el Comité Europeo de Protección de Datos en sus preguntas frecuentes, el uso de las BCRs para transferencias internacionales de datos a los Estados Unidos requiere también evaluar que se cumplan con las garantías adecuadas en materia de protección de datos, ya que la Ley estadounidense prevalece sobre el contenido de las BCRs.

Sobre las cláusulas contractuales tipo, debe incidirse en el hecho de que el TJUE ha declarado válida la ya mencionada Decisión 2010/87/UE, sin perjuicio de las cuestiones específicas planteadas. Y si las cláusulas contractuales tipo han sido adoptadas por la autoridad de protección de datos, tendrán que ser aprobadas por la Comisión. En cualquier caso, en relación con las citadas cláusulas el Comité Europeo de Protección de Datos ha señalado que es necesario llevar a cabo una evaluación o “assessment” de la situación y que en caso de que se concluya que teniendo en cuenta las diversas circunstancias del caso no es posible garantizar la transferencia esta debe ser suspendida. No obstante, si se considera que debe ser mantenida, deberá notificarse a la autoridad de protección de datos.

En cuanto a los códigos de conducta y mecanismos de certificación, será necesario esperar a que se aprueben los primeros, dado que a pesar de su previsión en el RGPD todavía no se han aplicado a las transferencias internacionales de datos.

---

<sup>13</sup>. *Ibid*, p. 11.



Por último, cabría atender también a las excepciones para situaciones específicas (art. 49 del RGPD), que requieren un análisis caso por caso. Estas excepciones son aplicables únicamente cuando no existe una decisión de adecuación o de otras garantías adecuadas y en cualquier caso de manera restrictiva, como ha indicado el Comité Europeo de Protección de Datos<sup>14</sup>.

## 9. Referencias

Sentencia del TJUE y conclusiones del Abogado General:

- [Sentencia del Tribunal de Justicia \(Gran Sala\)](#), de 16 de julio de 2020, asunto C-311/18.
- [Conclusiones del Abogado General](#), presentadas el 19 de diciembre de 2019.

Documentos de CMS:

- [Schrems strikes again: EU-US Privacy Shield invalid; Standard Contractual Clauses upheld but due diligence required](#).

Autoridades de protección de datos y otras fuentes:

- Agencia Española de Protección de Datos, [El Tribunal de Justicia de la Unión Europea declara inválido el Escudo de Privacidad para la realización de transferencias internacionales de datos a EEUU](#), 22 de Julio de 2020.
- *Commission nationale de l'informatique et des libertés (CNIL)* (Francia), [Invalidation du «Privacy shield»: la CNIL et ses homologues analysent actuellement ses conséquences](#), 17 juillet 2020.
- *Data Protection Commission* (Irlanda), [DPC statement on CJEU decision](#), 16 July 2020.
- *European Data Protection Board*, [Thirty-fourth Plenary session: Schrems II, Interplay PSD2 and GDPR and letter to MEP Ďuriš Nicholsonová on contact tracing, interoperability of apps and DPIAs](#), 20 July 2020.
  - [Statement on the CJUE Judgment in Case C-311/18](#), 17 July 2020.
  - [FAQs on Schrems II](#).
- *European Data Protection Supervisor*, [EDPS Statement following the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems \("Schrems II"\)](#), 17 July 2020.
- *European Commission*, [Opening remarks by Vice-President Jourová and Commissioner Reynders at the press point following the judgment in case C-311/18 Facebook Ireland and Schrems](#), 16 July 2020.
- *Federal Commissioner for Data Protection and Freedom of Information* (Alemania), [The BfDI's statement on the Schrems II judgment of the ECJ](#), 16 July 2020.
- *Information Commissioner's Office* (Reino Unido), [ICO statement on the judgment of the European Court of Justice in the Schrems II case](#), 16 July 2020.
- TJUE, [El Tribunal de Justicia invalida la Decisión 2016/1250 sobre la adecuación de la protección conferida por el Escudo de privacidad UE-EE.UU.](#), Comunicado de prensa nº 91/20, 16 de julio de 2020.
- *U.S. Department of State*, [European Court of Justice Invalidates EU-U.S. Privacy Shield](#), 17 July 2020.

---

14. Comité Europeo de Protección de Datos, [Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25 May 2018](#).



Para más información, puede contactar con el equipo de TMC de CMS Albiñana & Suárez de Lezo:



**Javier Torre de Silva**  
**Socio | TMC / Protección de Datos**

T +34 91 451 93 21  
E [javier.torredesilva@cms-asl.com](mailto:javier.torredesilva@cms-asl.com)



**José Luis Piñar**  
**Of Counsel | TMC / Protección de Datos**

T +34 91 451 40 53  
E [joseluis.pinar@cms-asl.com](mailto:joseluis.pinar@cms-asl.com)



**Miguel Recio**  
**Asociado | TMC / Protección de Datos**

T +34 91 452 01 90  
E [miguel.recio@cms-asl.com](mailto:miguel.recio@cms-asl.com)



La presente publicación no constituye asesoramiento jurídico de sus autores. Para más información:

[cms-asl@cms-asl.com](mailto:cms-asl@cms-asl.com) | [cms.law](http://cms.law)



Law . Tax

**Your free online legal information service.**

A subscription service for legal articles on a variety of topics delivered by email.

[cms-lawnow.com](http://cms-lawnow.com)

-----  
The information held in this publication is for general purposes and guidance only and does not purport to constitute legal or professional advice.

CMS Legal Services EEIG (CMS EEIG) is a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEIG provides no client services. Such services are solely provided by CMS EEIG's member firms in their respective jurisdictions. CMS EEIG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEIG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the member firms or their offices.

**CMS locations:**

Aberdeen, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Mexico City, Milan, Mombasa, Monaco, Moscow, Munich, Muscat, Nairobi, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Riyadh, Rome, Santiago de Chile, Sarajevo, Seville, Shanghai, Sheffield, Singapore, Skopje, Sofia, Strasbourg, Stuttgart, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

-----  
[cms.law](http://cms.law)

