

**Invalidación del
Privacy Shield:
guía sobre cómo
actuar ante
transferencias
internacionales
de datos a
Estados Unidos**

Informe

Área de Privacidad y Protección de Datos

El Tribunal de Justicia de la Unión Europea invalida el “Privacy Shield” y manifiesta sus reservas sobre las Cláusulas Contractuales Tipo

Recientemente conocíamos la Resolución del Tribunal de Justicia de la Unión Europea (en adelante “**TJUE**”) de fecha 16 de julio de 2020, correspondiente al caso Facebook Ireland vs. Schrems, en relación con el asunto C-311/18, mediante la que se invalida la Decisión de Ejecución (UE) 2016/1250 de la Comisión de 12 de julio de 2016, sobre la adecuación de la protección conferida por el Escudo de la Privacidad entre la Unión Europea y Estados Unidos (en adelante, “**Privacy Shield**”).

(I) ANÁLISIS SOBRE EL IMPACTO DE LA RESOLUCIÓN DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, MEDIANTE LA QUE SE INVALIDA PRIVACY SHIELD

La citada Resolución **afecta de forma directa a todas aquellas empresas, administraciones e instituciones que, directa o indirectamente, comuniquen o posibilitem el acceso a los datos personales a entidades estadounidenses adheridas a Privacy Shield ya sea en el marco de una prestación de servicios, al objeto de una cesión de datos o porque su empresa matriz u otras empresas del grupo a las que haya que reportar información con datos personales, tengan su sede en EEUU y la transferencia se hubiese regularizado en base al Privacy Shield**

La misma, que no establece un periodo de gracia para la adaptación efectiva de las empresas a la nueva situación, alcanza una serie de conclusiones en relación con las transferencias internacionales de datos derivadas de estas relaciones:

(i) Sobre la invalidación del Privacy Shield:

1. **El TJUE considera que es inválido**, como Decisión de adecuación, teniendo en cuenta que no garantiza el nivel mínimo de protección exigido por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante, “**RGPD**”).

Así, **el TJUE entiende que no cumple con los requisitos exigidos para la realización de transferencias basadas en una Decisión de adecuación**, ya que, **no se reconocen a los interesados, cuyos datos personales son transferidos fuera de la Unión Europea, sus derechos efectivos y exigibles, ni se establecen canales eficaces para la interposición de recursos administrativos y acciones judiciales que sean efectivos.**

2. Debe recordarse que las Decisiones de adecuación, parten de la necesidad de que no existan dudas sobre la equivalencia, en lo que se refiere al respeto de la protección de los datos, del marco jurídico imperante en el Estado del importador, en relación con el que resulte de aplicación en el Estado del exportador, es decir, que respete el contenido de Carta de los Derechos Fundamentales de la Unión Europea.

En este sentido, el TJUE entiende que, **la propia redacción de Privacy Shield establece la limitación al cumplimiento de los principios esenciales para el tratamiento de los datos personales de ciudadanos europeos, en los casos en los que fuera necesaria su revelación, a causa de los requerimientos formulados**



por las Autoridades estadounidenses, los cuales primarían sobre los principios establecidos en la normativa de protección de datos aplicable en la Unión Europea.

3. Esta limitación supone una **interferencia en los derechos y libertades reconocidos por la Carta de los Derechos Fundamentales** referenciada. Así, el TJUE establece que las interferencias derivadas de los programas de vigilancia basados en el artículo 702 de la *Foreign Intelligence Surveillance Act* y en la *Executive Order 12333*, no están cubiertas por los requisitos que aseguran, con sujeción al principio de proporcionalidad, un nivel de protección equivalente al garantizado por la Carta Europea, así como los programas de vigilancia basados en los términos de la *Presidential Policy Directive 28*, respecto de los cuales, el propio Gobierno de los Estados Unidos ha aceptado que no concede a los interesados derechos ejercitables ante los Tribunales contra las Autoridades de los estadounidenses.
4. Así, el TJUE concluye que la existencia de una legislación que no prevé ninguna posibilidad de que una persona física pueda interponer recursos judiciales para acceder a sus datos personales o para obtener la rectificación o la supresión de los mismos, no respeta el derecho fundamental a la tutela judicial efectiva, resultando incompatible con el nivel de protección exigido por el marco normativo de Unión Europea.
5. Adicionalmente, establece que la figura del Defensor del Pueblo no es suficiente para garantizar la protección legal de los interesados, ya que:
 - No es independiente, Toda vez que reporta al Secretario de Estado de Estados Unidos.
 - No tiene mecanismos para garantizar el cumplimiento por parte de los servicios de inteligencia.

(ii) Sobre la validez de las Cláusulas Contractuales Tipo:

1. El TJUE se pronuncia sobre las Cláusulas Contractuales Tipo para la transferencia de datos personales a encargados de tratamiento situados en terceros países (en adelante, "**CCT**"), modificadas por la Decisión de Ejecución (UE) 2016/2297 de la Comisión de 16 de diciembre de 2016, entendiéndose que, **si bien son válidas, en ocasiones será necesario aportar garantías adicionales.**

Así las cosas, entiende que su utilización implica la necesidad de garantizar un nivel protección equivalente al exigido por el RGPD, interpretado conjuntamente con la Carta Europea de Derechos Humanos. Sin embargo, **no sólo deberá tenerse en cuenta el contenido de las propias CCT, sino si el marco jurídico existente en el país de destino permite garantizar el referido cumplimiento.**

En este sentido, entre los aspectos a valorarse se encontrarían, si el tercer país cuenta con una normativa o garantía constitucional en relación con la protección de la privacidad y de los datos personales, su grado de desarrollo e implantación.

2. El TJUE entiende que dichas Cláusulas, al ser contractuales, **no vinculan a las Autoridades del país de destino, toda vez que las mismas no forman parte del acuerdo.** Por lo tanto, puede resultar que, incluso pese a la correcta suscripción de las mismas, no se considere que se han otorgado las garantías adecuadas, por no existir la certeza de que las Autoridades del estado del receptor de la información no puedan acceder a la información, ni que los interesados



dispongan de mecanismos legislativos eficaces para la defensa y ejercicio de sus derechos.

3. Como medida de control, el TJUE reconoce que **una Autoridad de Control debe prohibir/suspender una transferencia internacional de datos basada en CCT cuando no se garantice un nivel equivalente al del RGPD en el país de destino.**

Esta facultad de prohibición/suspensión, no debe entenderse como exclusiva de las Autoridades de Control, ya que se reconoce a los propios exportadores de la información, apoyados por los destinatarios, la posibilidad de anular las transferencias internacionales que se vinieran realizando cuando observasen que, por cualesquiera razones, no es posible garantizar el nivel de protección de datos personales equivalente al exigido por el RGPD.

En este marco **quedarían exceptuados aquellos países que ya cuentan con una Decisión de adecuación por parte de la Comisión Europea** (Suiza, Canadá, Argentina, Uruguay, Guernesey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda y Japón).

4. El TJUE establece que los **responsables y encargados del tratamiento, deberán abordar la definición y establecimiento de medidas adicionales, para la salvaguarda de las garantías adecuadas** y, sólo en caso subsidiario, deberá encargarse a la autoridad supervisora correspondiente, no determinándose en la Resolución la naturaleza de esas medidas adicionales que aporten garantías suficientes que no puedan ser menoscabadas, ni siquiera, por la propia autoridad del Estado receptor de la información.
5. Se recuerda la obligación establecida por las CCT de que, **el destinatario de la información, informe al responsable de cualquier impedimento que obste al cumplimiento de las mismas. Lo cual incluirá cualquier cambio normativo que considere, le puede impedir cumplir con las obligaciones establecidas en las CCT, por tener un efecto adverso sustancial en las garantías y obligaciones previstas en las mismas.** En estos casos, deberán devolverse la totalidad de los datos que hubiesen sido transferidos a ese tercer país con anterioridad debiendo, igualmente, devolverse o destruirse la totalidad de copias de los mismos, que constasen.

Así, **si el responsable no cesa en la transferencia internacional y decide seguir con la misma, deberá notificárselo a la Autoridad de Control competente a fin de que audite al destinatario y decida sobre si el contexto de la transferencia realizada aconseja la prohibición de la misma** por considerarse que no se garantiza un nivel de protección suficiente.

6. A modo aclaratorio cabe indicar que el TJUE realiza estas consideraciones con respecto a:
 - La Decisión de adecuación relativa al Privacy Shield que afecta a cualquier tipo de relación (Responsable de Tratamiento a Responsable del Tratamiento, Responsable del Tratamiento a Encargado del Tratamiento, entre otras)
 - La Decisión de la Comisión de 5 de febrero de 2010 que **únicamente regula la relación de Responsable del Tratamiento con un Encargado del Tratamiento.**

Dicho esto, las consideraciones arriba analizadas, así como las que se pasen a analizar, **aplicarían a cualquier tipo de relación independientemente de la consideración jurídica de cada parte.** El análisis realizado por el TJUE está



focalizado en la falta de seguridad de la normativa del país importador de los datos personales, por lo que **estas medidas y recomendaciones debieran aplicar indiferentemente a la relación existente** entre las partes.

(II) PRONUNCIAMIENTOS DE LAS AUTORIDADES DE CONTROL

A raíz de la Resolución del TJUE diferentes Autoridades en materia de protección de datos se han pronunciado en el sentido de cómo debe abordarse este nuevo escenario por parte de las empresas, administraciones e instituciones europeas, teniendo en cuenta, tanto su impacto en relación con la protección de los datos de los ciudadanos, como desde el punto de vista de las relaciones económicas entre Europa y Estados Unidos, valoradas en 7,1 billones de dólares y la adhesión de 5.300 empresas al sistema invalidado por el TJUE, en este sentido:

(i) Comité Europeo de Protección de Datos.

El Comité Europeo se ha manifestado, de forma muy somera, en relación con la necesidad de analizar en qué podrán consistir las medidas adicionales referenciadas en la presente Nota, En este sentido, con el fin de garantizar estos aspectos, establece la necesidad de que sea el exportador quien:

1. Lleve a cabo una evaluación (si es necesario con la asistencia del importador) de si los países a los que se envían los datos ofrecen una protección adecuada. Teniendo en cuenta:
 - a. El contenido de las CCT.
 - b. Las circunstancias específicas de la transferencia; así como
 - c. El régimen jurídico aplicable en el país del importador. Cuyo análisis se llevará a cabo a la luz de los factores no exhaustivos establecidos en el artículo 45.2 del RGPD.
2. Establezca medidas adicionales a las incluidas en las CCT, si el resultado de esta evaluación es que el país del importador no proporciona un nivel de protección esencialmente equivalente al establecido en la Unión Europea. Estas medidas no han sido informadas ni especificadas aún por este organismo.

(ii) Supervisor Europeo de Protección de Datos.

El Supervisor Europeo se ha pronunciado en similares términos, a través de su *DPS Statement following the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems*. En este sentido, celebra la decisión alcanzada por el TJUE respecto a la invalidez de Privacy Shield, resaltando la necesidad de reconocer la posibilidad de reclamar y/o ejercitar derechos.

Si bien reconoce la vigencia de las CCT, como medida para otorgar las garantías adecuadas para la realización de una transferencia internacional, en ausencia de una Decisión de adecuación, no ha aportado aún información adicional sobre las posibles medidas adicionales enunciadas por el TJUE.

(iii) Alemania.

El Comisionado Federal en su declaración sobre la Resolución analizada, ha destacado que las transferencias internacionales de datos siguen siendo posibles, debiendo adoptarse medidas especiales de protección para realizadas con Estados Unidos.



Por su parte la Autoridad de Berlín solicitó en su declaración que los responsables de tratamientos que realizaban transferencias internacionales de datos a Estados Unidos, los transfirieran a Europa, manteniendo un standard de seguridad jurídica hasta que se reforme el marco jurídico.

En relación con la utilización de CCT ha destacado la obligación de comprobar antes de la primera transferencia de datos si el tercer país tiene acceso estatal a los datos que va más allá de lo permitido por la legislación europea y si existen esos derechos de acceso, entre otros aspectos.

En este sentido, la Comisionada para la Protección de Datos y la Libertad de Información de Berlín, ha indicado que los responsables del tratamiento que transfieren datos personales a los Estados Unidos están ahora obligados a cambiar inmediatamente a proveedores de servicios en la Unión Europea o en un país con un nivel adecuado de protección de datos.

(iv) Holanda.

La Autoridad de Control Holandesa ha destacado que las organizaciones de la Unión Europea, por el momento, simplemente no deben transferir datos personales a Estados Unidos, señalando que la Comisión debe establecer un nuevo régimen para dichas transferencias.

(v) Irlanda.

La Autoridad irlandesa ha recalcado la necesidad de adoptar mecanismos que garanticen que las transferencias internacionales sean realizadas a países que cuenten con un nivel equivalente al de la Unión Europea, cuestionando la validez práctica de las propias CCT en tanto no pudieran garantizarse estas exigencias de forma efectiva.

(vi) Liechtenstein.

La autoridad de protección de datos en su declaración sobre la Resolución analizada informó que analizaría sus consecuencias para las transferencias de datos a terceros países y, además, publicaría nuevas instrucciones. Además, destacó que, hasta que se acuerde un nuevo instrumento con Estados Unidos, las empresas tendrán que basarse en las salvaguardias establecidas en el artículo 46 del RGPD, incluidas las CCT.

(vii) Otros Estados de la Unión Europea.

El resto de Autoridades de Control de los Estados de la Unión Europea, como es el caso de España, se han pronunciado en el sentido de que se encuentran analizando la Resolución, así como la necesidad de abordar nuevos mecanismos de manera conjunta y de revisar el impacto en otros mecanismos como las CCT.

(viii) Posición de Estados Unidos.

Por su relevancia en este asunto, debe tenerse en cuenta el pronunciamiento de la **Secretaría de Comercio de Estados Unidos**, que recalca el estrecho contacto con la Comisión Europea y el Comité Europeo de Protección de Datos, así como su intención de seguir administrando el programa del Privacy Shield, incluyendo el procesamiento de solicitudes de autocertificación y recertificación, entendiéndose que la Resolución del TJUE hoy no exime a las organizaciones incluidas de las obligaciones adquiridas previamente.



(III) CONCLUSIONES Y MODO DE PROCEDER PARA LA REGULARIZACIÓN DE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS A ESTADOS UNIDOS

Ante la situación actual, con el fin de poder analizar el impacto dentro de las empresas, administraciones e instituciones de la Resolución analizada, así como, como abordar la necesaria regularización de las transferencias internacionales de datos que pudieran estar realizando, puede concluirse:

1. El primer aspecto que debe recordarse es la **pérdida de vigencia del Privacy Shield, lo que impide la realización de transferencias internacionales a entidades establecidas en Estados Unidos, basadas en este mecanismo.**
2. De conformidad con lo establecido en el RGPD, en ausencia de una Decisión de adecuación o de garantías adecuadas, la transferencia o conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si cumple alguna de las excepciones siguientes:
 - **El interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas.**
 - La transferencia sea **necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado** (dicho tratamiento ha de ser estrictamente necesario para la realización de dicha relación, esto es, por ejemplo, una prestación de servicios contratada directamente con una entidad fuera del Espacio Económico Europeo).
 - La transferencia sea **necesaria para la celebración o ejecución de un contrato, en interés del interesado**, entre el responsable del tratamiento y otra persona física o jurídica (con la misma salvedad comentada anteriormente).
 - La transferencia sea **necesaria por razones importantes de interés público**. (el cual ha de estar debidamente justificado).
 - La transferencia **sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones**.
 - La transferencia sea **necesaria para proteger los intereses vitales del interesado o de otras personas**, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento.
 - La transferencia **se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo**, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.
3. Antes de realizar transferencias internacionales de datos, deberá **evaluarse si los países a los que se envían los datos ofrecen una protección adecuada**. En caso de no ser así, como mecanismo adicional a la firma de las Clausulas Contractuales Tipo, deberán aportarse medidas adicionales, que permitan garantizar dicho cumplimiento. En este sentido, el considerando 109 del RGPD recoge la posibilidad de modificación de las CCT siempre y cuando sea para ampliar las garantías y obligaciones determinadas por las mismas.



4. En ausencia de una Decisión de Adecuación, se deberán otorgar las garantías adecuadas previstas en la normativa vigente y concretamente en los artículos 44 a 49 del RGPD:
 - **Podrán ser utilizadas de las CCT, actualmente vigentes, incorporando garantías adicionales.**
 - **Establecimiento y aprobación de Normas Corporativas Vinculantes.**
 - **Códigos de conducta junto con compromisos vinculantes y exigibles** del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.
 - **Mecanismo de certificación aprobado** junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.
 - **Recurrir a las Autoridades de Control y solicitar la correspondiente autorización administrativa.**
5. Las empresas deberán **implementar mecanismos que puedan posibilitarles la obtención de dicha información de cara a evaluar la idoneidad del importador de los datos o de la realización de las posibles transferencias**, cuestiones que ya venían recogidas en el propio RGPD en relación con las garantías a analizar en los procesos de elección de proveedores.
6. **La definición e implantación de las garantías adicionales corresponden al exportador y al importador de los datos.** Aunque subsidiariamente la iniciativa podrá corresponder a la Autoridad de Control correspondiente.

Deberán, por ejemplo, establecer mecanismos de evaluación sobre la idoneidad y nivel de cumplimiento o sobre la necesaria actualización de las mismas conforme al criterio de las Autoridades europeas y posibles nuevas Decisiones europeas.

El propio RGPD en su Considerando 109 ya establece la posibilidad de que el responsable o el encargado del tratamiento recurran a las CCT incluyendo las mismas en un contrato más amplio, mediante un compromiso entre las partes, **añadiendo cláusulas o garantías adicionales, siempre que no contradigan, directa o indirectamente, las CCT adoptadas por la Comisión o por una Autoridad de Control, ni mermen los derechos o las libertades fundamentales de los interesados.**

En todo caso, la adopción de estas garantías adicionales debe ir encaminada a evitar que puedan concurrir los motivos que han generado la anulación de Privacy Shield, asegurando que se evite un acceso indebido a los datos personales por parte del tercer país y, que se garanticen mecanismos de defensa efectivos, tanto para el exportador, como para con los derechos de los afectados cuyos datos son objeto de transferencia internacional.

7. La no adopción de garantías suficientes **podrá dar lugar, junto a las posibles sanciones derivadas de llevar a cabo transferencias internacionales de datos sin las garantías suficientes, a la inmovilización o bloqueo de los datos, el derecho del interesado a recibir una indemnización por los daños y perjuicios sufridos**, así como el posible daño reputacional para las propias Empresas.
8. En caso de no regularizar las transferencias internacionales de datos, debemos recordar que, conforme al artículo 72 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos



digitales, será considerada como **infracción muy grave**, la **transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o a una organización internacional**, cuando no concurren las **garantías, requisitos o excepciones establecidos en el RGPD**, lo puede conllevar **sanciones económicas de hasta 4% volumen de negocio global o hasta los 20 millones de euros**.

**Área de Privacidad
y Protección de Datos**

+ 34 91 781 61 60

info@ecija.com

ECIJA



EXPANSIÓN
2016, 2017,
2018 y 2019

Proyecto más innovador
Mejor Firma de
Economía Digital



FINANCIAL
TIMES
2019

Entre las 20 Firmas
más innovadoras
de Europa



Banda 1 en TMT por
Chambers and
Partners y Legal 500

THE LAWYER

2019

Mejor Firma en TMT
de Europa



FORBES
2017

Mejor Firma de
Tecnología de España

Torre de Cristal
Pº de la Castellana, 259C
28046 Madrid