Translations proofread by EDPB Members.
This language version has not yet been proofread.

Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE

Adoptadas el 10 de noviembre de 2020

Resumen ejecutivo

El Reglamento general de protección de datos (RGPD) de la UE se adoptó con un doble propósito: facilitar la libre circulación de datos personales dentro de la Unión Europea, preservando al mismo tiempo los derechos y libertades fundamentales de las personas, en particular su derecho a la protección de los datos personales.

En su reciente sentencia C-311/18 (Schrems II), el Tribunal de Justicia de la Unión Europea (TJUE) nos recuerda que la protección otorgada a los datos personales en el Espacio Económico Europeo (EEE) debe acompañar a los datos dondequiera que vayan. La transferencia de datos personales a terceros países no puede ser un medio para socavar o reducir la protección otorgada en el EEE. El Tribunal también afirma lo anterior aclarando que el nivel de protección en terceros países no tiene por qué ser idéntico al garantizado en el EEE, sino esencialmente equivalente. El Tribunal defiende asimismo la validez de las cláusulas contractuales tipo como instrumento de transferencia que puede servir para garantizar contractualmente un nivel de protección esencialmente equivalente para los datos transferidos a terceros países.

Las cláusulas contractuales tipo y otros instrumentos de transferencia mencionados en el artículo 46 del RGPD no operan aisladamente. El Tribunal sostiene que los responsables o encargados del tratamiento, que actúan como exportadores, son responsables de verificar, de manera individualizada y, en su caso, en colaboración con el importador del tercer país, si la legislación o la práctica del tercer país afectan a la eficacia de las garantías apropiadas contenidas en los instrumentos de transferencia del artículo 46 del RGPD. En tales supuestos, el Tribunal deja abierta la posibilidad de que los exportadores apliquen medidas complementarias que palíen estas lagunas de protección, a fin de que esta alcance el nivel exigido por el Derecho de la Unión. El Tribunal no especifica qué medidas podrían ser. Sin embargo, el Tribunal subraya que los exportadores tendrán que determinarlas caso por caso. Tal extremo concuerda con el principio de responsabilidad proactiva del artículo 5, apartado 2, del RGPD, que exige que los responsables del tratamiento sean responsables y capaces de demostrar el cumplimiento de los principios del RGPD relativos al tratamiento de datos personales.

Para ayudar a los exportadores (ya sean responsables o encargados del tratamiento, entidades privadas u organismos públicos que traten datos personales en el ámbito de aplicación del RGPD) con la compleja tarea de evaluar a terceros países y de establecer medidas complementarias adecuadas cuando sea necesario, el Comité Europeo de Protección de Datos (CEPD) ha adoptado estas recomendaciones. Estas recomendaciones proporcionan a los exportadores una serie de pasos, posibles fuentes de información y algunos ejemplos de medidas complementarias que podrían aplicarse.

Como **primer paso**, el CEPD aconseja que usted, como exportador, **conozca sus transferencias**. Catalogar todas las transferencias de datos personales a terceros países puede resultar una tarea difícil. No obstante, es necesario saber dónde van los datos personales para garantizar que se les otorgue un nivel de protección esencialmente equivalente dondequiera que se traten. También se debe comprobar que los datos transferidos sean adecuados y pertinentes y se limiten a lo necesario en relación con los fines para los que se transfieren y tratan en el tercer país.

Un **segundo** paso consiste en **verificar el instrumento en el que se basa la transferencia** de entre los enumerados en el capítulo V del RGPD. Si la Comisión Europea ya ha declarado adecuado el país, la región o el sector al que se transfieren los datos a través de una de sus decisiones de adecuación en virtud del artículo 45 del RGPD o de la anterior Directiva 95/46, siempre que la decisión siga en vigor, no tendrá que adoptar ninguna otra medida aparte de supervisar que la decisión de adecuación

conserve su validez. En ausencia de una decisión de adecuación, deberá recurrir a uno de los instrumentos de transferencia enumerados en el artículo 46 del RGPD para las transferencias que sean periódicas y repetitivas. Solo en algunos casos de transferencias ocasionales y no repetitivas podrá acogerse a alguna de las excepciones previstas en el artículo 49 del RGPD, si cumple las condiciones.

Un **tercer paso** consiste en **evaluar** si hay algo en la **legislación o la práctica del tercer país** que pueda afectar a la eficacia de las garantías adecuadas de los instrumentos de transferencia en los que se basa, en el contexto de su transferencia específica. Su evaluación debe centrarse principalmente en la legislación de terceros países que sea pertinente para su transferencia y en el instrumento de transferencia del artículo 46 del RGPD en el que se está basando y que puede socavar su nivel de protección. Para evaluar los elementos que deben tenerse en cuenta al evaluar la legislación de un tercer país sobre el acceso a los datos por parte de las autoridades públicas a efectos de vigilancia, véanse las recomendaciones del CEPD sobre las garantías esenciales europeas. En particular, estos factores deben considerarse detenidamente cuando la legislación que regula el acceso a los datos por parte de las autoridades públicas sea ambigua o no se encuentre a disposición del público. En ausencia de una legislación que regule las circunstancias en las que las autoridades públicas pueden acceder a los datos personales, si aun así desea proceder a la transferencia, deberá examinar otros elementos pertinentes y objetivos y no confiar en factores subjetivos como la probabilidad de que las autoridades públicas accedan a sus datos de una manera que no se ajuste a las normas de la UE. Deberá llevar a cabo esta evaluación con la debida diligencia y documentarla cuidadosamente, ya que tendrá que rendir cuentas de la decisión que tome a raíz de ella.

Un **cuarto paso** consiste en **determinar y adoptar las medidas complementarias** necesarias para que el nivel de protección de los datos transferidos se ajuste a la norma de equivalencia esencial de la UE. Este paso solo es necesario si su evaluación revela que la legislación del tercer país afecta a la eficacia del instrumento de transferencia del artículo 46 del RGPD en el que se basa o al que tiene intención de recurrir en el contexto de su transferencia. Estas recomendaciones contienen (en el anexo 2) una lista no exhaustiva de ejemplos de medidas complementarias, con algunas de las condiciones necesarias para ser eficaces. Como ocurre con las garantías adecuadas contenidas en los instrumentos de transferencia del artículo 46, algunas medidas complementarias pueden ser eficaces en algunos países, pero no necesariamente en otros. Será responsable de evaluar su eficacia en el contexto de la transferencia, a la luz de la legislación del tercer país y del instrumento de transferencia en el que esté basándose, así como de la decisión que tome. Esto también podría exigir que se combinaran varias medidas complementarias. En última instancia, podría llegar a la conclusión de que ninguna medida complementaria puede garantizar un nivel de protección esencialmente equivalente para su transferencia específica. En los casos en los que no sea adecuada ninguna medida complementaria, deberá evitar, suspender o poner fin a la transferencia para no comprometer el nivel de protección de los datos personales. También deberá llevar a cabo esta evaluación de las medidas complementarias con la debida diligencia y documentarla.

Un **quinto paso** consiste en **adoptar** cualquier **fase de procedimiento formal** que pueda requerir su medida complementaria, en función del instrumento de transferencia del artículo 46 del RGPD en el que se esté basando. Estas recomendaciones especifican dichas formalidades. Es posible que tenga que consultar a sus autoridades de control competentes sobre algunas de ellas.

El **sexto y último paso** consistirá en que vuelva a evaluar a intervalos adecuados el nivel de protección de los datos que transfiere a terceros países y supervise si ha habido o se producirá algún cambio que pueda incidir en él. El principio de responsabilidad proactiva exige una vigilancia continua del nivel de protección de los datos personales.

Las autoridades de control seguirán ejerciendo su mandato de supervisar la aplicación del RGPD y de velar por su cumplimiento. Las autoridades de control tendrán debidamente en cuenta las medidas que adopten los exportadores para garantizar que los datos que transfieren gozan de un nivel de protección esencialmente equivalente. Como recuerda el Tribunal, las autoridades de control suspenderán o prohibirán las transferencias de datos en aquellos casos en los que, a raíz de una investigación o una denuncia, consideren que no puede garantizarse un nivel de protección esencialmente equivalente.

Las autoridades de control seguirán elaborando orientaciones para los exportadores y coordinando sus acciones en el CEPD para garantizar la coherencia en la aplicación de la legislación de la UE en materia de protección de datos.

Índice

El Comité Europeo de Protección de Datos

Visto el artículo 70, apartado 1, letra e), del 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 (en lo sucesivo, «RGPD»),

Visto el Acuerdo sobre el Espacio Económico Europeo (EEE) y, en particular, su anexo XI y su Protocolo 37, modificado por la Decisión del Comité Mixto del EEE n.º 154/2018, de 6 de julio de 2018[1],

Vistos los artículos 12 y 22 de su Reglamento interno,

Considerando lo siguiente:

(1) El Tribunal de Justicia de la Unión Europea (TJUE) concluye en su sentencia de 16 de julio de 2020, *Data Protection Commissioner/Facebook Ireland Limited y Maximillian Schrems*, C-311/18, que el artículo 46, apartados 1 y 2, letra c), del RGPD deben interpretarse en el sentido de que las garantías adecuadas, los derechos protegidos jurídicamente y las vías de recurso legales efectivas que exigen dichas disposiciones deben asegurar que los interesados cuyos datos personales se transfieran a un tercer país en virtud de cláusulas tipo de protección de datos reciban un nivel de protección sustancialmente equivalente al garantizado en la Unión por dicho Reglamento, leído en relación con la Carta de los Derechos Fundamentales de la Unión Europea.[2]

(2) Como ha subrayado el Tribunal, debe asegurarse un nivel de protección de las personas físicas esencialmente equivalente al garantizado en la Unión por el RGPD, interpretado a la luz de la Carta, con independencia de la disposición del capítulo V en virtud de la cual se lleve a cabo la transferencia de datos personales a un tercer país. Las disposiciones del capítulo V pretenden garantizar la continuidad de ese elevado nivel de protección cuando los datos personales se transfieren a un tercer país.[3]

(3) El considerando 108 y el artículo 46, apartado 1, del RGPD establecen que, en ausencia de una decisión de adecuación de la Unión, el responsable o el encargado del tratamiento deben adoptar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado. Un responsable o encargado del tratamiento podrá ofrecer garantías adecuadas, sin necesidad de una autorización específica de una autoridad de control, mediante el uso de uno de los instrumentos de transferencia enumerados en el artículo 46, apartado 2, del RGPD, como las cláusulas tipo de protección de datos.

[1] Las referencias a los «Estados miembros» realizadas en el presente documento deben entenderse como referencias a los «Estados miembros del EEE».
[2] Sentencia del TJUE de 16 de julio de 2020, *Data Protection Commissioner/Facebook Ireland Limited y Maximillian Schrems [en lo sucesivo*, C-311/18 (Schrems II)], segunda conclusión.
[3] C-311/18 (Schrems II), apartados 92 y 93.

(4) El Tribunal aclara que las cláusulas tipo de protección de datos adoptadas por la Comisión tienen únicamente por objeto proporcionar garantías contractuales que se apliquen de manera uniforme en todos los terceros países a los responsables y encargados del tratamiento establecidos en la Unión Europea. Debido a su naturaleza contractual, las cláusulas tipo de protección de datos no pueden vincular a las autoridades públicas de terceros países, ya que no son partes en el contrato. Por consiguiente, es posible que los exportadores de datos tengan que completar las garantías contenidas en dichas cláusulas tipo de protección de datos con medidas adicionales para garantizar el cumplimiento del nivel de protección exigido por el Derecho de la Unión en un tercer país en concreto. El Tribunal hace referencia al considerando 109 del RGPD, que menciona esta posibilidad e insta a los responsables y encargados del tratamiento a utilizarla.[4]

(5) El Tribunal declaró que corresponde ante todo al exportador de datos comprobar, de manera individualizada y, en su caso, en colaboración con el importador de los datos, si el Derecho del tercer país de destino garantiza un nivel de protección esencialmente equivalente, con arreglo al Derecho de la Unión, de los datos personales transferidos en virtud de las cláusulas tipo de protección de datos, estableciendo, en su caso, medidas complementarias a las que ofrecen dichas cláusulas.[5]

(6) Si el responsable o el encargado del tratamiento establecidos en la Unión Europea no están en condiciones de adoptar las medidas complementarias adecuadas para garantizar un nivel de protección sustancialmente equivalente con arreglo al Derecho de la Unión, los mismos o, en su defecto, la autoridad de control competente, estarán obligados a suspender o poner fin a la transferencia de datos personales al tercer país de que se trate.[6]

(7) Ni el RGPD ni el Tribunal definen o especifican las «garantías adicionales», las «medidas adicionales» o las «medidas complementarias» a las garantías de los instrumentos de transferencia enumerados en el artículo 46, apartado 2, del RGPD que los responsables y encargados del tratamiento pueden adoptar para asegurarse del cumplimiento del nivel de protección exigido por el Derecho de la Unión en un tercer país en concreto.

(8) El CEPD ha decidido, por iniciativa propia, examinar esta cuestión y proporcionar a los responsables y encargados del tratamiento, que actúan como exportadores, recomendaciones sobre el proceso que pueden seguir para identificar y adoptar medidas complementarias. Estas recomendaciones tienen por objeto proporcionar una metodología para que los exportadores determinen si sería necesario aplicar medidas adicionales a sus transferencias y, en caso afirmativo, cuáles. Es responsabilidad primordial de los exportadores garantizar que los datos transferidos reciben en el tercer país un nivel de protección sustancialmente equivalente al garantizado en la Unión. Con estas recomendaciones, el CEPD pretende fomentar una aplicación coherente del RGPD y de la sentencia del Tribunal, de conformidad con el mandato del CEPD.[7]

HA ADOPTADO LA SIGUIENTE RECOMENDACIÓN:

[4] C-311/18 (Schrems II), apartados 132 y 133.
[5] C-311/18 (Schrems II), apartado 134.
[6] C-311/18 (Schrems II), apartado 135.
[7] Artículo 70, apartado 1, letra e), del RGPD.

1 RESPONSABILIDAD PROACTIVA EN LAS TRANSFERENCIAS DE DATOS

1. El Derecho primario de la Unión considera que el derecho a la protección de datos es un derecho fundamental.[8] En consecuencia, el derecho a la protección de datos goza de un elevado nivel de protección y solo pueden imponerse limitaciones si están previstas por la ley, respetan el contenido esencial de su derecho, son proporcionadas y necesarias y responden efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.[9] El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.[10]

2. Para asegurar que no se menoscabe el nivel de protección otorgado por el RGPD, un nivel de protección sustancialmente equivalente al garantizado en la UE debe acompañar a los datos cuando se transfieran a terceros países fuera del EEE.

3. El derecho a la protección de datos tiene un carácter activo. Exige a los exportadores e importadores (ya sean responsables o encargados del tratamiento) que vayan más allá de un reconocimiento o un cumplimiento pasivo de este derecho.[11] Los responsables y encargados del tratamiento deben tratar de respetar el derecho a la protección de datos de manera activa y continua mediante la aplicación de medidas jurídicas, técnicas y organizativas que garanticen su eficacia. Los responsables y encargados del tratamiento también deben ser capaces de demostrar estos esfuerzos a los interesados, al público en general y a las autoridades de control de la protección de datos. Este es el denominado principio de responsabilidad proactiva o de rendición de cuentas.[12]

4. El principio de responsabilidad proactiva, que es necesario para garantizar la aplicación efectiva del nivel de protección que confiere el RGPD, también se aplica a las transferencias de datos a terceros países[13], ya que son una forma de tratamiento de datos en sí mismas.[14] Como subrayó el Tribunal en su sentencia, debe asegurarse un nivel de protección sustancialmente equivalente al garantizado en la Unión por el RGPD interpretado a la luz de la Carta, con independencia de la disposición de dicho capítulo en virtud de la cual se lleve a cabo una transferencia de datos personales a un tercer país.[15]

5. En la sentencia Schrems II, el Tribunal hace hincapié en la responsabilidad de los exportadores e importadores de garantizar que el tratamiento de datos personales se ha realizado y seguirá realizándose respetando el nivel de protección establecido por el Derecho de la Unión en materia de protección de datos, y de suspender la transferencia o rescindir el contrato cuando el importador de los datos no pueda cumplir o haya dejado de cumplir las cláusulas tipo de protección de datos incorporadas en el contrato pertinente entre el exportador y el importador.[16] El responsable o el

[8] Artículo 8, apartado 1, de la Carta de los Derechos Fundamentales y artículo 16, apartado 1, del TFUE, considerando 1, artículo 1, apartado 2, del RGPD.
[9] Artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea.
[10] Considerando 4 del RGPD y C-507/17 Google LLC, que se ha subrogado en los derechos de Google Inc.,/Commission nationale de l'informatique et des libertés (CNIL), apartado 60.
[11] C-92/09 y C-93/02, Volker und Markus Schecke GbR/Land Hessen, Conclusiones de la Abogado General Sharpston, 17 de junio de 2010, apartado 71.
[12] Artículo 5, apartado 2, y artículo 28, apartado 3, letra h), del RGPD.
[13] Artículo 44 y considerando 101 del RGPD, así como artículo 47, apartado 2, letra d), del RGPD.
[14] Sentencia del TJUE de 6 de octubre de 2015, *Maximillian Schrems/Data Protection Commissioner [en lo sucesivo* C-362/14 (Schrems I)], apartado 45.
[15] C-311/18 (Schrems II), apartados 92 y 93.
[16] C-311/18 (Schrems II), apartados 134, 135, 139, 140, 141 y 142.

encargado del tratamiento que actúen como exportadores deben garantizar que los importadores colaboran con el exportador, en su caso, en el ejercicio de estas responsabilidades, manteniéndole informado, por ejemplo, de cualquier novedad que afecte al nivel de protección de los datos personales recibidos en el país del importador.[17] Estas responsabilidades son una aplicación del principio del RGPD de responsabilidad proactiva a las transferencias de datos.[18]

2 PLAN DE TRABAJO: APLICACIÓN EN LA PRÁCTICA DEL PRINCIPIO DE RESPONSABILIDAD PROACTIVA A LAS TRANSFERENCIAS DE DATOS

6. A continuación se presenta un plan de trabajo con las medidas que deben tomarse para averiguar si usted (el exportador de datos) debe instaurar medidas complementarias para poder transferir datos legalmente fuera del EEE. «Usted» en el presente documento significa el responsable o encargado del tratamiento que actúa como exportador de datos y que trata datos personales en el ámbito de aplicación del RGPD, incluido el tratamiento por parte de entidades privadas y organismos públicos al transferir datos a organismos privados.[19] En cuanto a las transferencias de datos personales efectuadas entre organismos públicos, se ofrecen orientaciones específicas en las *Directrices 2/2020 sobre el artículo 46, apartado 2, letra a), y el artículo 46, apartado 3, letra b), del Reglamento n.º 2016/679 para las transferencias de datos personales entre autoridades y organismos públicos del EEE y terceros países*.[20]

7. Deberá documentar adecuadamente esta evaluación y las medidas complementarias que seleccione y aplique, así como poner dicha documentación a disposición de la autoridad de control competente, previa solicitud.[21]

2.1 Paso 1: conocer sus transferencias

8. Para saber qué puede necesitar usted (el exportador de datos) para poder continuar con sus transferencias de datos personales o realizar otras nuevas[22], el primer paso es asegurarse de que es plenamente consciente de sus transferencias y las conoce. Registrar y catalogar todas las transferencias puede ser un ejercicio complejo para las entidades que participan en transferencias múltiples, diversas y periódicas con terceros países y que utilizan una serie de encargados y subencargados. Conocer las transferencias es un primer paso esencial para cumplir sus obligaciones en virtud del principio de responsabilidad proactiva.

[17] C-311/18 (Schrems II), apartado 134.
[18] Artículo 5, apartado 2, y artículo 28, apartado 3, letra h), del RGPD.
[19] Véanse las Directrices 3/2018 del CEPD relativas al ámbito territorial del RGPD (artículo 3) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_es
[20] Directrices 2/2020 del CEPD sobre el artículo 46, apartado 2, letra a), y el artículo 46, apartado 3, letra b), del Reglamento n.º 2016/679 para las transferencias de datos personales entre autoridades y organismos públicos del EEE y terceros países; véase (en inglés) https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en
[21] Artículo 5, apartado 2, del RGPD y artículo 24, apartado 1, del RGPD.
[22] Tenga en cuenta que el acceso remoto de una entidad de un tercer país a datos situados en el EEE también se considera una transferencia.

9. Para tener pleno conocimiento de sus transferencias, puede basarse en los registros de las actividades de tratamiento que puede estar obligado a mantener como responsable o encargado del tratamiento en virtud del artículo 30 del RGPD.[23] Las acciones previas para cumplir las obligaciones de informar a los interesados con arreglo al artículo 13, apartado 1, letra f), y el artículo 14, apartado 1, letra f), del RGPD sobre sus transferencias de datos personales a terceros países también pueden ayudarle.[24]

10. Al catalogar las transferencias, no olvide tener también en cuenta las transferencias ulteriores, por ejemplo, si sus encargados del tratamiento fuera del EEE transfieren los datos personales que usted les confió a un subencargado del tratamiento en otro tercer país o en el mismo.[25]

11. En consonancia con el principio del RGPD de «minimización de los datos»,[26] deberá verificar que los datos transferidos son adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se transfieren y tratan en el tercer país.

12. Estas actividades deben llevarse a cabo antes de efectuar cualquier transferencia y actualizarse antes de reanudarlas tras la suspensión de las operaciones de transferencia de datos: debe saber dónde pueden los importadores localizar o tratar los datos personales que haya exportado (mapa de destinos).

13. Tenga en cuenta que el acceso remoto desde un tercer país (por ejemplo, en el ámbito de operaciones de asistencia) o el almacenamiento en una nube situada fuera del EEE también se consideran transferencias.[27] Más concretamente, si utiliza una infraestructura internacional en nube, deberá evaluar si sus datos se transferirán a terceros países y a cuáles, a menos que el proveedor de la nube indique claramente en su contrato que los datos no se tratarán en absoluto en terceros países.

2.2 Paso 2: determinar los instrumentos de transferencia en los que se está basando

[23] Véase el artículo 30 del RGPD y, en concreto, su apartado 1, letra e), y apartado 2, letra c). Además, sus registros de tratamiento deben contener una descripción de sus actividades de tratamiento (incluidas, a título meramente ilustrativo, las categorías de interesados, las categorías de datos personales y los fines del tratamiento, así como información específica sobre las transferencias de datos). Algunos responsables y encargados del tratamiento están exentos de la obligación de mantener registros del tratamiento (artículo 30, apartado 5, del RGPD). Para obtener orientaciones sobre esta exención, véase el Grupo de Trabajo del artículo 29, Documento de posición sobre las excepciones a la obligación de mantener registros de las actividades de tratamiento de conformidad con el artículo 30, apartado 5, del RGPD (aprobado por el CEPD el 25 de mayo de 2018).

[24] Con arreglo a las normas de transparencia del RGPD, deberá informar a los interesados sobre las transferencias de datos personales a terceros países [artículo 13, apartado 1, letra f), y artículo 14, apartado 1, letra f), del RGPD]. En particular, deberá informarles de la existencia o ausencia de una decisión de adecuación por parte de la Comisión Europea o, en el caso de las transferencias a que se refieren los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, del RGPD, hacer referencia a las garantías adecuadas u oportunas y a los medios por los que se puede obtener una copia de las mismas o dónde se han puesto a su disposición. La información facilitada al interesado debe ser correcta y actual, especialmente a la luz de la jurisprudencia del Tribunal en materia de transferencias.

[25] Cuando el responsable del tratamiento haya concedido su autorización previa, específica o general, por escrito, de conformidad con el artículo 28, apartado 2, del RGPD.

[26] Artículo 5, apartado 1, letra c), del RGPD.

[27] Véase la pregunta frecuente n.º 11: «*debe tenerse en cuenta que incluso proporcionar acceso a datos desde un tercer país, por ejemplo a efectos administrativos, también equivale a una transferencia*», Preguntas frecuentes del CEPD sobre la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311/18, Data Protection Commissioner/Facebook Ireland Limited y Maximillian Schrems, 23 de julio de 2020.

14. Un segundo paso que deberá dar es identificar los instrumentos de transferencia en los que se está basando de entre los que enumera y prevé el capítulo V del RGPD.

Decisiones de adecuación

15. La Comisión Europea puede reconocer, a través de sus **decisiones de adecuación** relativas a algunos o a todos los terceros países a los que transfiere datos personales, que estos ofrecen un nivel adecuado de protección de los datos personales.[28]

16. El efecto de tal decisión de adecuación es que los datos personales podrán transmitirse del EEE a ese tercer país sin necesidad de un instrumento de transferencia de los plasmados en el artículo 46 del RGPD.

17. Las decisiones de adecuación pueden abarcar un país en su conjunto o limitarse a una parte del mismo. Las decisiones de adecuación pueden abarcar todas las transferencias de datos a un país o limitarse a algunos tipos de transferencias (por ejemplo, en un sector).[29]

18. La Comisión Europea publica la lista de sus decisiones de adecuación en su sitio web.[30]

19. Si transfiere datos personales a terceros países, regiones o sectores cubiertos por una decisión de adecuación de la Comisión (en la medida en que proceda), **no tendrá que adoptar ninguna otra medida, como se describe en estas recomendaciones.**[31] No obstante, deberá seguir supervisando si las decisiones de adecuación relativas a sus transferencias se revocan o invalidan.[32]

20. Sin embargo, las decisiones de adecuación no impiden a los interesados presentar una reclamación. Tampoco impiden a las autoridades de control acudir a un órgano jurisdiccional nacional si albergan dudas sobre la validez de una decisión, de modo que un órgano jurisdiccional nacional puede plantear una cuestión prejudicial al Tribunal de Justicia de la Unión Europea con el fin de examinar dicha validez.[33]

---

[28] La Comisión Europea tiene competencias para determinar, sobre la base del artículo 45 del RGPD, si un país no perteneciente a la UE ofrece un nivel adecuado de protección de datos. Del mismo modo, la Comisión Europea tiene competencias para determinar si una organización internacional ofrece un nivel de protección adecuado.

[29] Artículo 45, apartado 1, del RGPD.

[30] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[31] Siempre que usted y el importador de datos hayan aplicado medidas para cumplir las demás obligaciones en virtud del RGPD; en caso contrario, se aplicarán dichas medidas.

[32] La Comisión Europea debe revisar periódicamente todas las decisiones de adecuación y supervisar si los terceros países beneficiarios de las decisiones de adecuación siguen garantizando un nivel de protección adecuado (véase el artículo 45, apartados 3 y 4, del RGPD). Asimismo, el TJUE puede invalidar las decisiones de adecuación [véanse sus sentencias en los asuntos C-362/14 (Schrems I) y C-311/18 (Schrems II)].

[33] C-311/18 (Schrems II), apartados 118 a 120. Las autoridades de control no podrán ignorar la decisión de adecuación y suspender o prohibir las transferencias de datos personales a dichos países alegando únicamente la insuficiencia del nivel de protección. Solo podrán ejercer su facultad de suspender o prohibir las transferencias de datos personales a ese tercer país por otros motivos (por ejemplo, medidas de seguridad insuficientes que infrinjan el artículo 32 del RGPD o ninguna base jurídica que sustente válidamente el tratamiento de datos, infringiendo así el artículo 6 del RGPD). Las autoridades de control podrán examinar, con total independencia, si la transferencia de esos datos cumple los requisitos establecidos en el RGPD y, en su caso, interponer un recurso ante los órganos jurisdiccionales nacionales para que, si albergan dudas sobre la validez de la decisión de adecuación de la Comisión, presenten una petición de decisión prejudicial ante el Tribunal de Justicia de la Unión Europea a efectos de examinar su validez.

Ejemplo: un ciudadano de la UE, el Sr. Schrems, presentó una reclamación en junio de 2013 ante la Data Protection Commission (DPC) de Irlanda y pidió a esta autoridad de control que prohibiera o suspendiera la transferencia de sus datos personales de Facebook Ireland a Estados Unidos, ya que consideraba que el Derecho y la práctica de Estados Unidos no garantizaban una protección adecuada de los datos personales almacenados en su territorio contra las actividades de vigilancia realizadas por las autoridades públicas. La DPC desestimó la reclamación, alegando, en particular, que en la Decisión 2000/520 la Comisión Europea consideró que, en el marco del régimen de «puerto seguro», Estados Unidos garantizaba un nivel adecuado de protección de los datos personales transferidos (la Decisión de puerto seguro). El Sr. Schrems impugnó la resolución de la DPC y la High Court irlandesa planteó al Tribunal de Justicia de la Unión Europea (TJUE) una cuestión sobre la validez de la Decisión 2000/520. Posteriormente, el TJUE decidió invalidar la Decisión 2000/520 de la Comisión sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada.[34]

Instrumentos de transferencia del artículo 46 del RGPD

21. El artículo 46 del RGPD enumera una serie de instrumentos de transferencia que contienen «*garantías adecuadas*» que los exportadores pueden utilizar para transferir datos personales a terceros países en ausencia de decisiones de adecuación. Los principales tipos de instrumentos de transferencia del artículo 46 del RGPD son:

    - cláusulas tipo de protección de datos (CPT);
    - normas corporativas vinculantes (NCV);
    - códigos de conducta;
    - mecanismos de certificación;
    - cláusulas contractuales específicas.

22. Sea cual sea el instrumento de transferencia del artículo 46 del RGPD que elija, deberá garantizar que, en general, los datos personales transferidos disfruten de un nivel de protección esencialmente equivalente.

23. El artículo 46 del RGPD contiene principalmente garantías adecuadas de carácter contractual que pueden aplicarse a las transferencias a todos los terceros países. La situación en el tercer país al que usted transfiere los datos puede seguir requiriendo que complemente estos instrumentos de transferencia y las garantías que contienen con medidas adicionales («medidas complementarias») para garantizar un nivel de protección esencialmente equivalente.[35]

Excepciones

24. Además de las decisiones de adecuación y de los instrumentos de transferencia del artículo 46 del RGPD, este contiene una tercera vía que permite la transferencia de datos personales en determinadas situaciones. Con sujeción a condiciones específicas, podrá seguir transfiriendo datos personales sobre la base de una excepción enumerada en el artículo 49 del RGPD.

[34] Asunto C-362/14 (Schrems I).
[35] C-311/18 (Schrems II), apartados 130 y 133. Véase también el apartado 2.3 siguiente.

25. El artículo 49 del RGPD tiene carácter excepcional. Las excepciones que contiene deben interpretarse de manera restrictiva y están relacionadas fundamentalmente con actividades de tratamiento ocasionales y no repetitivas. El CEPD ha publicado sus Directrices 2/2018 sobre las excepciones contempladas en el artículo 49 del Reglamento 2016/679. [36]

26. Antes de acogerse a una excepción del artículo 49 del RGPD, deberá comprobar si su transferencia cumple las estrictas condiciones que esta disposición establece para cada una de ellas.

***

27. Si su transferencia no puede basarse legalmente en una decisión de adecuación ni en una excepción del artículo 49, deberá continuar con el paso 3.

2.3 Paso 3: evaluar si el instrumento de transferencia del artículo 46 del RGPD en el que se está basando es eficaz a la luz de todas las circunstancias de la transferencia

28. La selección de un instrumento de transferencia del artículo 46 del RGPD puede no ser suficiente. El instrumento de transferencia debe garantizar que el nivel de protección garantizado por el RGPD no se vea menoscabado por la transferencia.[37] En otras palabras, su instrumento de transferencia debe ser eficaz en la práctica.

29. Por eficacia se entiende que los datos personales transferidos gocen en el tercer país de un nivel de protección sustancialmente equivalente al garantizado en el EEE.[38] Este no es el caso si se impide al importador de datos cumplir sus obligaciones en virtud del instrumento de transferencia del artículo 46 del RGPD elegido debido al Derecho y las prácticas del tercer país aplicables a la transferencia.

30. Por lo tanto, debe evaluar, en su caso en colaboración con el importador, si hay algún elemento del Derecho o la práctica del tercer país que pueda afectar a la eficacia de las garantías adecuadas del instrumento de transferencia del artículo 46 del RGPD en el que se está basando, en el contexto de su transferencia específica. En su caso, el importador de datos debe facilitarle las fuentes e información pertinentes sobre el tercer país en el que está establecido y la legislación aplicable a la transferencia. También puede hacer referencia a otras fuentes de información, como las enumeradas de forma no exhaustiva en el anexo 3.[39]

31. Su evaluación debe tener en cuenta a todos los agentes que participan en la transferencia (por ejemplo, responsables, encargados y subencargados del tratamiento de datos en el tercer país), identificados en el ejercicio de catalogación de las transferencias. Cuantos más responsables, encargados o importadores participen, más compleja será su evaluación. También tendrá que tener en cuenta en esta evaluación cualquier transferencia ulterior que pueda producirse.

32. A tal fin, deberá examinar las características de cada una de sus transferencias y determinar cómo se les aplica el ordenamiento jurídico interno del país al que se transfieren (o se transferirán ulteriormente) los datos.

---

[36] Para obtener más información al respecto, véase https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-22018-derogations-article-49-under-regulation_es.
[37] Artículo 44 del RGPD.
[38] C-311/18 (Schrems II), apartado 105 y segunda conclusión.
[39] Véase también el apartado 43 más adelante.

33. El contexto jurídico aplicable dependerá de las circunstancias de la transferencia, en particular:

- fines para los que se transfieren y tratan los datos (por ejemplo, comercialización, recursos humanos, almacenamiento, asistencia informática, ensayos clínicos);
- tipos de entidades que participan en el tratamiento (públicas/privadas; responsable/encargado);
- sector en el que tiene lugar la transferencia (por ejemplo, tecnología publicitaria, telecomunicaciones, finanzas, etc.);
- categorías de datos personales transferidos (por ejemplo, los datos personales relativos a los menores pueden entrar en el ámbito de aplicación de legislación específica del tercer país);
- si los datos se almacenarán en el tercer país o si solo existe un acceso remoto a los datos almacenados en la UE o el EEE;
- formato de los datos que se transferirán (es decir, en texto sencillo/seudonimizado o cifrado[40]);
- posibilidad de que los datos puedan ser objeto de transferencias ulteriores del tercer país a otro tercer país.[41]

34. Entre las leyes aplicables, tendrá que evaluar si alguna de ellas afecta a los compromisos contenidos en el instrumento de transferencia del artículo 46 del RGPD que ha elegido. Deberá comprobar si los compromisos que permiten a los interesados ejercer sus derechos en el contexto de transferencias internacionales (como las solicitudes de acceso, rectificación y supresión de datos transferidos) pueden cumplirse efectivamente en la práctica y no se ven frustrados por la ley en el tercer país de destino.

35. Tendrá que evaluar las normas pertinentes de carácter general en la medida en que repercutan en la aplicación efectiva de las garantías contenidas en el instrumento de transferencia del artículo 46 del RGPD y en los derechos fundamentales de las personas físicas (en particular, el derecho de recurso concedido al interesado en caso de acceso de las autoridades públicas de terceros países a los datos transferidos).

36. En cualquier caso, deberá prestar especial atención a las leyes pertinentes, en particular las que establecen requisitos para divulgar datos personales a las autoridades públicas o conceden a dichas autoridades poderes de acceso a los datos personales (por ejemplo, con fines de aplicación del Derecho penal, supervisión reglamentaria y seguridad nacional). Si estos requisitos o facultades se limitan a lo que es necesario y proporcionado en una sociedad democrática,[42] no pueden afectar a los compromisos contenidos en el instrumento de transferencia del artículo 46 del RGPD en el que usted se está basando.

[40] Algunos terceros países no permiten la importación de datos cifrados.
[41] Cuando el responsable del tratamiento haya concedido su autorización previa, específica o general, por escrito, de conformidad con el artículo 28, apartado 2, del RGPD.
[42] Véanse los artículos 47 y 52 de la Carta de los Derechos Fundamentales de la UE, el artículo 23, apartado 1, del RGPD y las Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia, de 10 de noviembre de 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

37. Las normas de la UE, como los artículos 47 y 52 de la Carta de los Derechos Fundamentales de la Unión Europea, deben utilizarse como referencia para evaluar si dicho acceso por parte de las autoridades públicas se limita a lo que es necesario y proporcionado en una sociedad democrática y si se concede a los interesados un recurso efectivo.

38. Al llevar a cabo esta evaluación, también son pertinentes diferentes aspectos del ordenamiento jurídico de ese tercer país, por ejemplo, los elementos enumerados en el artículo 45, apartado 2, del RGPD.[43] Por ejemplo, la situación del Estado de Derecho en un tercer país puede ser pertinente para evaluar la eficacia de los mecanismos disponibles para que las personas puedan obtener un recurso (judicial) contra el acceso ilegal de las autoridades a los datos personales. La existencia de una ley de protección de datos exhaustiva o de una autoridad independiente de protección de datos, así como la adhesión a los instrumentos internacionales que establecen garantías de protección de datos, pueden contribuir a garantizar la proporcionalidad de la injerencia gubernamental.[44]

***

39. Las recomendaciones del CEPD sobre garantías esenciales europeas (GEE) proporcionan elementos que deben evaluarse para determinar si el marco jurídico que rige el acceso a los datos personales por parte de las autoridades públicas de un tercer país, como las agencias de seguridad nacionales o las autoridades policiales, puede considerarse o no una injerencia justificable (y, por tanto, que no afecta a los compromisos asumidos en el instrumento de transferencia del artículo 46 del RGPD). En particular, estos factores deben considerarse detenidamente cuando la legislación que regula el acceso a los datos por parte de las autoridades públicas sea ambigua o no se encuentre a disposición del público.

40. Aplicadas a la situación de las transferencias de datos basadas en los instrumentos de transferencia del artículo 46, las recomendaciones del CEPD sobre garantías esenciales europeas pueden orientar al exportador y al importador de datos a la hora de evaluar si tales facultades injieren injustificadamente en las obligaciones del importador de datos de garantizar una equivalencia esencial.

41. La falta de un nivel de protección esencialmente equivalente será especialmente evidente cuando el Derecho o la práctica del tercer país pertinentes para su transferencia no cumplan los requisitos de las garantías esenciales europeas.

42. Su evaluación deberá basarse, ante todo, en la legislación a disposición del público. Sin embargo, en algunas situaciones esto no será suficiente porque puede faltar la legislación de los terceros países. En este caso, si sigue planteándose la transferencia, deberá examinar otros factores pertinentes y objetivos[45], y no confiar en los subjetivos, como la probabilidad de que las autoridades públicas accedan a sus datos de una manera contraria a las normas de la Unión. Deberá llevar a cabo esta evaluación con la debida diligencia y documentarla cuidadosamente, ya que tendrá que rendir cuentas de la decisión que tome a raíz de ella.[46]

[43] C-311/18 (Schrems II), apartado 104.

[44] Por ejemplo: el Convenio 108 (Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, STCE n.º 108) o el Convenio 108+ (Convenio modernizado para la protección de las personas con respecto al tratamiento de datos de carácter personal, STCE n.º 223) establecen vías de recurso legales internacionales aplicables en caso de violaciones de la protección de datos y contribuyen a proporcionar un nivel mínimo de protección de los datos personales y respeto de la vida privada.

[45] Véase el apartado 43 siguiente, así como el anexo 3.

[46] Artículo 5, apartado 2, del RGPD.

43. Puede completar su evaluación con información obtenida de otras fuentes[47], tales como:

- elementos que demuestren que una autoridad de un tercer país tratará de acceder a los datos con o sin el conocimiento del importador de datos, a la luz de los precedentes, el Derecho y las prácticas notificados;
- elementos que demuestren que una autoridad de un tercer país podrá acceder a los datos a través del importador de datos o mediante la interceptación directa del canal de comunicación a la luz de los precedentes notificados, las competencias legales y los recursos técnicos, financieros y humanos a su disposición.

44. Su evaluación puede, en última instancia, revelar que el instrumento de transferencia del artículo 46 del RGPD en el que se está basando y las garantías adecuadas que contiene:

- garantizan efectivamente que los datos personales transferidos gozarán en el tercer país de un nivel de protección sustancialmente equivalente al otorgado en el EEE. El Derecho y las prácticas del tercer país aplicables a la transferencia ponen al importador de datos en condiciones de cumplir sus obligaciones en virtud del instrumento de transferencia elegido. Deberá volver a evaluarlo a intervalos adecuados o cuando se produzcan cambios significativos (véase el paso 6).
- No garantizan efectivamente un nivel de protección esencialmente equivalente. El importador de datos no puede cumplir sus obligaciones debido al Derecho o las prácticas del tercer país aplicables a la transferencia. El TJUE subrayó que, cuando los instrumentos de transferencia del artículo 46 del RGPD no son suficientes, es responsabilidad del exportador de datos establecer medidas complementarias eficaces o no transferir los datos personales.[48]

El TJUE sostuvo, por ejemplo, que el artículo 702 de la FISA estadounidense no respeta las garantías mínimas derivadas del principio de proporcionalidad establecido en el Derecho de la Unión y no puede considerarse que se limite a lo estrictamente necesario. Esto significa que el nivel de protección de los programas autorizados por el artículo 702 de la FISA no es esencialmente equivalente a las garantías exigidas por el Derecho de la Unión. Por consiguiente, si el importador de datos o cualquier otro destinatario al que el importador de datos pueda divulgar los datos entran en el ámbito de aplicación del artículo 702 de la FISA[49], las CPT u otros instrumentos de transferencia del artículo 46 del RGPD solo podrán utilizarse para dicha transferencia si medidas técnicas adicionales hacen imposible o ineficaz el acceso a los datos transferidos.

[47] Véase también el anexo 3.
[48] TJUE C-311/18 (Schrems II), apartados 134 y 135.
[49] El artículo 702 de la FISA es aplicable si los datos se obtienen «de un proveedor de servicios de comunicaciones electrónicas o con la ayuda de este» [artículo 702 de la FISA = USC, título 50, artículo 1881a, apartado (h)(2)(A)(vi)], que a su vez se define en USC, título 50, artículo 1881, apartado (b)(4) como
«(A) un operador de telecomunicaciones, tal como se define en el artículo 153 del título 47;
(B) un proveedor de servicios de comunicaciones electrónicas, tal como se define en el artículo 2510 del título 18;
(C) un proveedor de un servicio informático a distancia, tal como se define en el artículo 2711 del título 18;
(D) cualquier otro proveedor de servicios de comunicaciones que tenga acceso a comunicaciones alámbricas o electrónicas, ya sea durante su transmisión o su almacenamiento; o
(E) un directivo, empleado o agente de una entidad descrita en los puntos (A), (B), (C) o (D)».

2.4 Paso 4: adoptar medidas complementarias

45. Si su evaluación en el marco del paso 3 ha revelado que su instrumento de transferencia del artículo 46 del RGPD no es eficaz, tendrá que considerar, en su caso en colaboración con el importador, si existen medidas complementarias que, si se añaden a las garantías contenidas en los instrumentos de transferencia, podrían garantizar que los datos transferidos se beneficiaran en el tercer país de un nivel de protección esencialmente equivalente al garantizado en la Unión.[50] Por definición, las «medidas complementarias» complementan las garantías que ya ofrece el instrumento de transferencia del artículo 46 del RGPD.[51]

46. Deberá identificar, caso por caso, qué medidas complementarias podrían ser eficaces para un conjunto de transferencias a un tercer país específico cuando se utilice un instrumento de transferencia concreto del artículo 46 del RGPD. Podrá basarse en sus evaluaciones anteriores en virtud de los pasos 1, 2 y 3 que anteceden y cotejar sus conclusiones con la eficacia potencial de las medidas complementarias para garantizar el nivel de protección requerido.

47. En principio, las medidas complementarias pueden tener un carácter contractual, técnico u organizativo. La combinación de diversas medidas de forma que se apoyen y fortalezcan mutuamente puede mejorar el nivel de protección y, por tanto, contribuir a cumplir las normas de la Unión.

48. Las medidas contractuales y organizativas por sí solas no impedirán en general el acceso a los datos personales por parte de las autoridades públicas del tercer país (cuando ello injiera injustificadamente en las obligaciones del importador de datos de garantizar una equivalencia esencial). De hecho, habrá situaciones en las que solo las medidas técnicas puedan impedir o hacer ineficaz el acceso de las autoridades públicas de terceros países a los datos personales, en particular con fines de vigilancia.[52] En tales situaciones, las medidas contractuales u organizativas pueden complementar las medidas técnicas y reforzar el nivel general de protección de los datos, obstaculizando por ejemplo los intentos de las autoridades públicas de acceder a los datos de una manera no conforme con las normas de la Unión.

49. En su caso, en colaboración con el importador de datos, podrá consultar la siguiente lista (no exhaustiva) de factores para determinar qué medidas complementarias serían más eficaces para proteger los datos transferidos:

    - formato de los datos que se transferirán (es decir, en texto sencillo/seudonimizado o cifrado);
    - naturaleza de los datos;
    - duración y complejidad del flujo de trabajo del tratamiento de datos, número de agentes que intervienen en el tratamiento y relación entre ellos [por ejemplo, si las transferencias implican a múltiples responsables del tratamiento o a responsables y encargados del tratamiento, o implicación de encargados que transferirán los datos de usted a su importador de datos

[50] C-311/18 (Schrems II), apartado 96.
[51] Considerando 109 del RGPD y C-311/18 (Schrems II), apartado 133.
[52] Cuando dicho acceso vaya más allá de lo necesario y proporcionado en una sociedad democrática; véanse los artículos 47 y 52 de la Carta de los Derechos Fundamentales de la Unión Europea, el artículo 23, apartado 1, del RGPD y las Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia, de 10 de noviembre de 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

(teniendo en cuenta las disposiciones pertinentes que les son aplicables con arreglo al Derecho del tercer país de destino)];[53]

- posibilidad de que los datos puedan ser objeto de transferencias ulteriores dentro del mismo tercer país o incluso a otros terceros países (por ejemplo, participación de subencargados del importador de datos[54]).

Ejemplos de medidas complementarias

50. En las listas no exhaustivas descritas en el anexo 2 pueden encontrarse algunos ejemplos de medidas técnicas, contractuales y organizativas que podrían estudiarse.

***

51. Si ha establecido medidas complementarias eficaces, que, junto con su instrumento de transferencia del artículo 46 del RGPD elegido, alcanzan un nivel de protección que ahora es esencialmente equivalente al nivel de protección garantizado en el EEE, sus transferencias pueden llevarse a cabo.

52. Cuando no sea capaz de encontrar o aplicar medidas complementarias eficaces que garanticen que los datos personales transferidos gozan de un nivel de protección esencialmente equivalente,[55] no deberá empezar a transferir datos personales al tercer país de que se trate sobre la base del instrumento de transferencia del artículo 46 del RGPD en el que se está basando. Si ya está realizando transferencias, deberá suspender o poner fin a la transferencia de datos personales.[56] De conformidad con las garantías incluidas en el instrumento de transferencia del artículo 46 del RGPD en el que se está basando, el importador deberá devolver o destruir en su totalidad los datos que ya haya transferido a ese tercer país y las copias de los mismos.[57]

Ejemplo: el Derecho del tercer país prohíbe las medidas complementarias que ha determinado (por ejemplo, prohíbe el uso del cifrado) o impide de otro modo su eficacia. No deberá empezar a transferir datos personales a este país o deberá detener las transferencias en curso al mismo.

53. Si decide continuar con la transferencia a pesar de que el importador no puede cumplir los compromisos contraídos en el instrumento de transferencia del artículo 46 del RGPD, deberá notificarlo a la autoridad de control competente de conformidad con las disposiciones específicas introducidas en el instrumento de transferencia pertinente del artículo 46 del RGPD.[58] La autoridad de

[53] El RGPD asigna obligaciones distintas a los responsables y a los encargados del tratamiento. Las transferencias pueden ser entre responsables, entre responsables conjuntos, de controlador a encargado y, previa autorización del responsable, de encargado a responsable o entre encargados.

[54] Véase la nota a pie de página 25.

[55] Cuando dicho acceso vaya más allá de lo necesario y proporcionado en una sociedad democrática; véanse los artículos 47 y 52 de la Carta de los Derechos Fundamentales de la Unión Europea, el artículo 23, apartado 1, del RGPD y las Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia, de 10 de noviembre de 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[56] C-311/18 (Schrems II), apartado 135.

[57] Véase la cláusula 12 del anexo de la Decisión 87/2010 relativa a las CPT; véase la cláusula de resolución extraordinaria (opcional) en el anexo B de la Decisión 2004/915/CE.

[58] Véanse las preguntas frecuentes del CEPD sobre la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311/18, Data Protection Commissioner/Facebook Ireland Limited y Maximillian Schrems, adoptadas el 23 de julio de 2020 y, en particular, las preguntas frecuentes 5, 6 y 9. Véase también la cláusula 4, letra g), de la Decisión 2010/87/UE de la Comisión, la cláusula 5, letra a), de la Decisión 2001/497/CE de la Comisión y la cláusula II, letra c), del anexo «Conjunto II» de la Decisión 2004/915/CE de la Comisión.

control competente suspenderá o prohibirá las transferencias de datos en aquellos casos en los que considere que no puede garantizarse un nivel de protección esencialmente equivalente.[59]

54. La autoridad de control competente podrá imponer cualquier otra medida correctora (por ejemplo, una multa) si, a pesar de que no puede demostrar un nivel de protección esencialmente equivalente en el tercer país, inicia o continúa la transferencia.

2.5 Paso 5: fases del procedimiento si ha determinado medidas complementarias eficaces

55. Las fases de procedimiento que puede tener que adoptar en caso de que haya determinado medidas complementarias eficaces que vayan a aplicarse pueden diferir en función del instrumento de transferencia del artículo 46 del RGPD que esté utilizando o tenga previsto utilizar.

2.5.1 Cláusulas tipo de protección de datos (CPT) [artículo 46, apartado 2, letras c) y d), del RGPD]

56. Cuando tenga intención de instaurar medidas complementarias además de las CPT, no es necesario que solicite una autorización a la autoridad de control competente para añadir este tipo de cláusulas o garantías adicionales, siempre que las medidas complementarias identificadas no contravengan, directa ni indirectamente, las CPT y sean suficientes para garantizar que no se menoscaba el nivel de protección garantizado por el RGPD.[60] El exportador y el importador de datos deberán garantizar que las cláusulas adicionales no puedan interpretarse en modo alguno en el sentido de que restringen los derechos y obligaciones de las CPT o reducen de cualquier otra forma el nivel de protección de datos. Deberá ser capaz de demostrar tal extremo, incluida la precisión de todas las cláusulas, de conformidad con el principio de responsabilidad proactiva y su obligación de proporcionar un nivel suficiente de protección de datos. Las autoridades de control competentes estarán facultadas para revisar estas cláusulas complementarias cuando sea necesario (por ejemplo, en caso de reclamación o de investigación por iniciativa propia).

57. Si tiene intención de modificar las propias cláusulas tipo de protección de datos o cuando las medidas complementarias añadidas «contravengan» directa o indirectamente las CPT, ya no se considerará que se está basando en cláusulas contractuales tipo[61] y deberá solicitar una autorización a la autoridad de control competente de conformidad con el artículo 46, apartado 3, letra a), del RGPD.

---

[59] C-311/18 (Schrems II), apartados 113 y 121.

[60] El considerando 109 del RGPD es del tenor siguiente: «La posibilidad de que el responsable o el encargado del tratamiento recurran a cláusulas tipo de protección de datos adoptadas por la Comisión o una autoridad de control no debe obstar a que los responsables o encargados incluyan las cláusulas tipo de protección de datos en un contrato más amplio, como un contrato entre dos encargados, o a que añadan otras cláusulas o garantías adicionales, siempre que no contradigan, directa o indirectamente, las cláusulas contractuales tipo adoptadas por la Comisión o por una autoridad de control, ni mermen los derechos o las libertades fundamentales de los interesados». Se proporcionan disposiciones similares en conjuntos de CPT adoptadas por la Comisión Europea en virtud de la Directiva 95/45/CE.

[61] Véase, por analogía, el Dictamen 17/2020 del CEPD sobre el proyecto de cláusulas contractuales tipo remitido por la autoridad de control de Eslovenia (artículo 28, apartado 8, del RGPD) acerca de las CPT del artículo 28 ya adoptadas, que contiene una disposición similar («Por otra parte, el Comité recuerda que la posibilidad de usar CPT adoptadas por una autoridad de control no es impedimento para que las partes añadan otras cláusulas o garantías adicionales, siempre que estas no contravengan, directa o indirectamente, las CPT adoptadas ni causen un perjuicio a los derechos o las libertades fundamentales de los interesados. Además, cuando se modifiquen las

2.5.2 NCV [artículo 46, apartado 2, letra b), del RGPD]

58. El razonamiento expuesto en la sentencia Schrems II también se aplica a otros instrumentos de transferencia con arreglo al artículo 46, apartado 2, del RGPD, ya que todos estos instrumentos son básicamente de naturaleza contractual, por lo que las garantías previstas y los compromisos asumidos por las partes no pueden vincular a las autoridades públicas de terceros países.[62]

59. La sentencia Schrems II es pertinente para las transferencias de datos personales sobre la base de las NCV, ya que el Derecho de terceros países puede afectar a la protección que ofrecen dichos instrumentos. El impacto exacto de la sentencia Schrems II en las NCV sigue siendo objeto de debate. El CEPD facilitará cuanto antes más detalles sobre la posible necesidad de incluir compromisos adicionales en las NCV en las referencias WP256/257.[63]

60. El Tribunal destacó que es responsabilidad del exportador y del importador de los datos evaluar si el nivel de protección exigido por el Derecho de la Unión se respeta en el país tercero de que se trate para determinar si las garantías proporcionadas por las CPT o las NCV pueden cumplirse en la práctica. Si este no es el caso, deberá evaluar si puede proporcionar medidas complementarias para garantizar un nivel de protección equivalente al establecido en el EEE, y si el Derecho o la práctica del país tercero no afectarán a estas medidas complementarias para evitar su efectividad.

2.5.3 Cláusulas contractuales específicas [artículo 46, apartado 3, letra a), del RGPD]

61. El razonamiento expuesto en la sentencia Schrems II también se aplica a otros instrumentos de transferencia con arreglo al artículo 46, apartado 2, del RGPD, ya que todos estos instrumentos son básicamente de naturaleza contractual, por lo que las garantías previstas y los compromisos contraídos por las partes no pueden vincular a las autoridades públicas de terceros países.[64] Por lo tanto, la sentencia Schrems II es pertinente para las transferencias de datos personales sobre la base de cláusulas contractuales específicas, ya que el Derecho de terceros países puede afectar a la protección que ofrecen dichos instrumentos. El impacto exacto de la sentencia Schrems II en las cláusulas específicas sigue siendo objeto de debate. El CEPD proporcionará más detalles lo antes posible.

2.6 Paso 6: volver a evaluar a intervalos adecuados

62. Deberá hacer un seguimiento continuo y, en su caso, en colaboración con los importadores de datos, de la evolución en el tercer país al que haya transferido datos personales que pueda afectar a su evaluación inicial del nivel de protección y a las decisiones que haya tomado en consecuencia sobre sus transferencias. La responsabilidad proactiva es una obligación permanente (artículo 5, apartado 2, del RGPD).

---

cláusulas de protección de datos tipo, dejará de considerarse que las partes han suscrito las CPT adoptadas»), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_es.pdf.

[62] TJUE, C-311/18 (Schrems II), apartado 132.

[63] Grupo de Trabajo del artículo 29, Documento de trabajo por el que se establece un cuadro con los elementos y principios que figuran en las normas corporativas vinculantes, revisado por última vez y adoptado el 6 de febrero de 2018, WP 256 rev. 01; Grupo de Trabajo del artículo 29, Documento de trabajo por el que se establece un cuadro con los elementos y principios que figuran en las normas corporativas vinculantes, revisado por última vez y adoptado el 6 de febrero de 2018, WP 257 rev. 01.

[64] TJUE, C-311/18 (Schrems II), apartado 132.

63. Deberá poner en marcha mecanismos suficientemente sólidos para asegurarse de que suspende o pone fin inmediatamente a las transferencias cuando:

- el importador haya incumplido o no pueda cumplir los compromisos que ha asumido en el instrumento de transferencia del artículo 46 del RGPD;
- las medidas complementarias ya no sean eficaces en ese tercer país.

3 CONCLUSIÓN

64. El RGPD establece normas sobre el tratamiento de datos personales en el EEE y, al hacerlo, permite la libre circulación de datos personales en el EEE. El capítulo V del RGPD regula las transferencias de datos personales a terceros países y establece una condición necesaria: la transferencia no debe menoscabar el nivel de protección de las personas físicas garantizado por el RGPD (artículo 44 del RGPD). La sentencia del TJUE C-311/18 (Schrems II) subraya la necesidad de garantizar la continuidad del nivel de protección que ofrece el RGPD a los datos personales transferidos a un tercer país.[65]

65. Para garantizar un nivel de protección de sus datos esencialmente equivalente, será ante todo necesario que conozca exhaustivamente sus transferencias. También deberá comprobar que los datos transferidos son adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se transfieren y tratan en el tercer país.

66. También deberá determinar el instrumento de transferencia en el que se está basando para las transferencias. Si el instrumento de transferencia no es una decisión de adecuación, deberá verificar caso por caso si el Derecho o la práctica del tercer país de destino menoscaban o no las garantías contenidas en el instrumento de transferencia del artículo 46 del RGPD en el contexto de sus transferencias. Cuando el instrumento de transferencia del artículo 46 del RGPD no logre por sí solo para los datos personales transferidos un nivel de protección esencialmente equivalente, las medidas complementarias pueden paliar la deficiencia.

67. Si no es capaz de encontrar o aplicar medidas complementarias eficaces que garanticen que los datos personales transferidos gozan de un nivel de protección esencialmente equivalente, no deberá empezar a transferir datos personales al tercer país de que se trate sobre la base del instrumento de transferencia que haya elegido. Si ya está realizando transferencias, se le pedirá que suspenda o ponga fin inmediatamente a la transferencia de datos personales.

68. La autoridad de control competente está facultada para suspender o poner fin a las transferencias de datos personales al tercer país si no se garantiza la protección de los datos transferidos que exige el Derecho de la Unión, en particular los artículos 45 y 46 del RGPD y la Carta de los Derechos Fundamentales.

Por el Comité Europeo de Protección de Datos

La Presidenta

(Andrea Jelinek)

[65] C-311/18 (Schrems II), apartado 93.

ANEXO 1: DEFINICIONES

- «Tercer país»: cualquier país que no sea un Estado miembro del EEE.
- «EEE»: el Espacio Económico Europeo, que incluye a los Estados miembros de la Unión Europea y a Islandia, Noruega y Liechtenstein. El RGPD se aplica al mismo en virtud del Acuerdo EEE, en particular su anexo XI y su Protocolo 37.
- «RGPD»: Reglamento (UE) n.º 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).
- «La Carta»: Carta de los Derechos Fundamentales de la Unión Europea, DO C 326 de 26 de octubre de 2012, pp. 391 a 407.
- «TJUE» o «el Tribunal»: se refieren al Tribunal de Justicia de la Unión Europea. Constituye la autoridad judicial de la Unión Europea y, en cooperación con los órganos jurisdiccionales de los Estados miembros, garantiza la aplicación y la interpretación uniformes del Derecho de la Unión.
- «Exportador de datos»: el responsable o encargado del tratamiento dentro del EEE que transfiere datos personales a un responsable o encargado del tratamiento de un tercer país.
- «Importador de datos»: el responsable o encargado del tratamiento en un tercer país que recibe u obtiene acceso a los datos personales transferidos desde el EEE.
- «Instrumento de transferencia del artículo 46 del RGPD»: hace referencia a las garantías adecuadas en virtud del artículo 46 del RGPD que los exportadores de datos deben instaurar al transferir datos personales a un tercer país en ausencia de una decisión de adecuación, de conformidad con el artículo 45, apartado 3, del RGPD. El artículo 46, apartados 2 y 3, del RGPD contiene la lista de instrumentos de transferencia que los responsables y encargados del tratamiento pueden utilizar.
- «CPT»: cláusulas tipo de protección de datos (o «cláusulas contractuales tipo») adoptadas por la Comisión Europea para las transferencias de datos personales entre responsables o encargados del tratamiento en el EEE y responsables o encargados fuera del EEE. Las cláusulas contractuales tipo adoptadas por la Comisión Europea son un instrumento de transferencia en virtud del RGPD, de conformidad con el artículo 46, apartado 2, letra c), y apartado 5, del RGPD.

ANEXO 2: EJEMPLOS DE MEDIDAS COMPLEMENTARIAS

69. Las siguientes medidas son ejemplos de medidas complementarias que podría considerar cuando alcance el paso 4, «adoptar medidas complementarias». Esta relación no es exhaustiva. Seleccionar y aplicar una o varias de estas medidas no garantizará necesaria y sistemáticamente que su transferencia cumple la norma de equivalencia esencial que exige el Derecho de la Unión. Deberá seleccionar las medidas complementarias que puedan garantizar efectivamente dicho nivel de protección para sus transferencias.

70. Cualquier medida complementaria solo podrá considerarse eficaz en el sentido de la sentencia del TJUE «Schrems II» en la medida en que aborde las deficiencias específicas detectadas en su evaluación de la situación jurídica en el tercer país. Si, en última instancia, no puede garantizar un nivel de protección esencialmente equivalente, no deberá transferir los datos personales.

71. Como responsable o encargado del tratamiento, es posible que se le exija que aplique algunas de las medidas descritas en el presente anexo, incluso si su importador de datos está cubierto por una decisión de adecuación, al igual que se le puede exigir que las aplique cuando trate datos dentro del EEE.[66]

Medidas técnicas

72. En esta sección se describen de manera no exhaustiva ejemplos de medidas técnicas, que pueden complementar las garantías que figuran en el artículo 46 del RGPD para asegurar el cumplimiento del nivel de protección requerido por el Derecho de la Unión en el contexto de una transferencia de datos personales a un tercer país. Estas medidas serán especialmente necesarias cuando la legislación de dicho país imponga a los importadores de datos obligaciones que sean contrarias a las garantías del artículo 46 del RGPD y puedan, en particular, afectar a la garantía contractual de un nivel de protección esencialmente equivalente contra el acceso de las autoridades públicas de ese tercer país a dichos datos.[67]

73. En aras de una mayor claridad, esta sección especifica, en primer lugar, las medidas técnicas que podrían ser eficaces en determinados supuestos o casos de uso para garantizar un nivel de protección esencialmente equivalente. La sección continúa con algunos supuestos/casos de uso en los que no se han encontrado medidas técnicas para garantizar dicho nivel de protección.

Supuestos para los que se pueden encontrar medidas *eficaces*

74. Las medidas enumeradas a continuación tienen por objeto garantizar que el acceso de las autoridades públicas de terceros países a los datos transferidos no afecte a la eficacia de las garantías apropiadas contenidas en los instrumentos de transferencia del artículo 46 del RGPD. Estas medidas se aplican incluso si el acceso de las autoridades públicas se ajusta al Derecho del país del importador, cuando dicho acceso vaya más allá de lo necesario y proporcionado en una sociedad democrática.[68] Estas

[66] Artículo 5 , apartado 2, y artículo 32 del RGPD.
[67] C-311/18 (Schrems II), apartado 135.
[68] Véanse los artículos 47 y 52 de la Carta de los Derechos Fundamentales de la Unión Europea, el artículo 23, apartado 1, del RGPD y las recomendaciones del CEPD sobre las garantías esenciales europeas para medidas de vigilancia.

medidas tienen por objeto evitar la posible vulneración del acceso impidiendo a las autoridades identificar a los interesados, inferir información sobre ellos, individualizarlos en otro contexto o asociar los datos transferidos con otros conjuntos de datos que puedan poseer y que puedan contener, entre otros datos, identificadores en línea proporcionados por los dispositivos, aplicaciones, herramientas y protocolos utilizados por los interesados en otros contextos.

75. Las autoridades públicas de terceros países pueden tratar de acceder a los datos transferidos

a) En tránsito, accediendo a las líneas de comunicación utilizadas para transmitir los datos al país receptor. Este acceso puede ser pasivo, en cuyo caso el contenido de la comunicación, posiblemente tras un proceso de selección, simplemente se copiará. No obstante, el acceso también puede ser activo en el sentido de que las autoridades públicas se interpongan en el proceso de comunicación no solo leyendo el contenido, sino también manipulando o suprimiendo partes del mismo.

b) Durante su custodia por un destinatario previsto de los datos, bien accediendo a las propias instalaciones de tratamiento, bien exigiendo que el destinatario de los datos localice y extraiga datos de interés y los remita a las autoridades.

76. En esta sección se examinan supuestos en los que se aplican medidas eficaces en ambos casos. Si el Derecho del país receptor solo prevé un tipo de acceso, podrían aplicarse diferentes medidas complementarias y ser suficientes en las circunstancias concretas de una transferencia en particular. Por lo tanto, es necesario que el exportador de datos analice cuidadosamente, con el apoyo del importador de datos, las obligaciones impuestas a este último.

Por ejemplo, los importadores de datos estadounidenses que entran en el ámbito de aplicación del título 50, artículo 1881a, del USC (artículo 702 de la FISA) están obligados directamente a conceder acceso a los datos personales importados que obren en su poder, custodia o control, o a entregarlos. Esto puede hacerse extensivo a cualquier clave criptográfica necesaria para que los datos sean inteligibles.

77. Los supuestos describen circunstancias específicas y las medidas adoptadas. Cualquier cambio en los supuestos puede dar lugar a conclusiones diferentes.

78. Es posible que los responsables del tratamiento tengan que aplicar algunas o todas las medidas aquí descritas, independientemente del nivel de protección previsto por la legislación aplicable al importador de datos, por ser necesarias para cumplir lo dispuesto en los artículos 25 y 32 del RGPD en las circunstancias concretas de la transferencia. En otras palabras, los exportadores podrían verse obligados a aplicar las medidas descritas en el presente documento aunque sus importadores de datos estén cubiertos por una decisión de adecuación, al igual que los responsables y encargados del tratamiento pueden verse obligados a aplicarlas cuando los datos se tratan dentro del EEE.

Caso de uso 1: almacenamiento de datos para copias de seguridad y otros fines que no requieran el acceso a los datos sin cifrar

79. Un exportador de datos utiliza a un proveedor de servicios de alojamiento de datos en un tercer país para almacenar datos personales, por ejemplo, con fines de copia de seguridad.

Si

1. los datos personales se tratan mediante un cifrado fuerte antes de su transmisión,

2. el algoritmo de cifrado y su parametrización (por ejemplo, longitud de clave, modo de funcionamiento, si procede) se ajustan al estado de la técnica y pueden considerarse sólidos contra el criptoanálisis realizado por las autoridades públicas del país receptor, teniendo en cuenta los recursos y las capacidades técnicas (por ejemplo, la capacidad informática para ataques de fuerza bruta) de que disponen,
3. la fuerza del cifrado tiene en cuenta el período específico durante el cual debe preservarse la confidencialidad de los datos personales cifrados,
4. el algoritmo de cifrado se aplica sin defectos mediante programas informáticos adecuadamente conservados cuya conformidad con la especificación del algoritmo elegido se ha verificado, por ejemplo, mediante una certificación,
5. las claves se gestionan (generan, administran, almacenan, si procede, vinculan a la identidad del destinatario previsto y revocan) de forma fiable, y
6. las claves se conservan únicamente bajo el control del exportador de datos u otras entidades a las que se haya encomendado esta tarea domiciliadas en el EEE o en un tercer país, territorio o uno o varios sectores específicos de un tercer país, o en una organización internacional para la que la Comisión haya establecido, de conformidad con el artículo 45 del RGPD, que se garantiza un nivel de protección adecuado,

el CEPD considerará que el cifrado realizado constituye una medida complementaria eficaz.

Caso de uso 2: transferencia de datos seudonimizados

80. Un exportador de datos seudonimiza primero los datos que posee y luego los transfiere a un tercer país para su análisis, por ejemplo, con fines de investigación.

Si

1. un exportador de datos transfiere datos personales tratados de tal manera que los datos personales ya no puedan atribuirse a un interesado concreto ni utilizarse para individualizar al interesado en un grupo más amplio, sin utilizar información adicional,[69]
2. dicha información adicional obra exclusivamente en poder del exportador de datos y se conserva por separado en un Estado miembro o en un tercer país, territorio o uno o varios sectores específicos de un tercer país, o en una organización internacional para la que la Comisión haya establecido, de conformidad con el artículo 45 del RGPD, que se garantiza un nivel de protección adecuado,
3. se impide la divulgación o el uso no autorizado de dicha información adicional mediante las garantías técnicas y organizativas adecuadas, se asegura que el exportador de datos conserva el control exclusivo del algoritmo o del repositorio que permite la reidentificación utilizando la información adicional, y
4. el responsable del tratamiento ha comprobado, mediante un análisis exhaustivo de los datos en cuestión, teniendo en cuenta cualquier información que las autoridades públicas del país receptor puedan poseer, que los datos personales seudonimizados no pueden atribuirse a una persona física identificada o identificable, ni siquiera realizando una referencia cruzada a dicha información,

[69] En consonancia con el artículo 4, apartado 5, del RGPD: «"seudonimización": el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable».

el CEPD considerará que la seudonimización llevada a cabo constituye una medida complementaria eficaz.

81. Obsérvese que, en muchas situaciones, los factores específicos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de una persona física, su ubicación física o su interacción con un servicio basado en Internet en momentos concretos[70] pueden permitir la identificación de dicha persona incluso si se omiten su nombre, dirección u otros identificadores sencillos.

82. Esto es especialmente cierto cuando los datos se refieren al uso de servicios de información (tiempo de acceso, secuencia de características a las que se accede, características del dispositivo utilizado, etc.). Estos servicios podrían estar sujetos, al igual que para el importador de datos personales, a la obligación de conceder acceso a las mismas autoridades públicas de su jurisdicción, que probablemente estarán en posesión de datos sobre el uso de dichos servicios de información por parte de la persona o personas a las que se dirigen.

83. Además, dado que el uso de algunos servicios de información es público por su propia naturaleza, o es posible su explotación por partes con recursos sustanciales, los responsables del tratamiento tendrán que prestar especial atención, teniendo en cuenta que es probable que las autoridades públicas de su jurisdicción posean datos sobre el uso de los servicios de información por parte de la persona a la que se dirigen.

Caso de uso 3: datos cifrados que simplemente transitan por terceros países

84. Un exportador de datos desea transferir datos a un destino que se ha reconocido que ofrece una protección adecuada de conformidad con el artículo 45 del RGPD. Los datos se canalizan a través de un tercer país.

Si

1. un exportador de datos transfiere datos personales a un importador de datos en una jurisdicción que garantiza una protección adecuada, los datos se transportan por Internet y pueden canalizarse geográficamente a través de un tercer país que no ofrece un nivel de protección esencialmente equivalente,
2. se utiliza un cifrado del transporte respecto del cual se garantiza que los protocolos de cifrado empleados son de última generación y ofrecen una protección eficaz contra los ataques activos y pasivos con los recursos que se sabe obran en poder de las autoridades públicas del tercer país,
3. el descifrado solo es posible fuera del tercer país en cuestión,
4. las partes implicadas en la comunicación acuerdan una autoridad o infraestructura de certificación de clave pública fiable,
5. se utilizan las medidas específicas de protección más modernas contra ataques activos y pasivos al transporte cifrado,
6. en caso de que el cifrado del transporte no ofrezca por sí mismo la seguridad adecuada debido a la experiencia con las vulnerabilidades de la infraestructura o del *software* utilizado, los datos

[70] Artículo 4, apartado 1, del RGPD: «"datos personales"»: toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona».

personales también están cifrados de extremo a extremo en la capa de aplicación utilizando métodos de cifrado más avanzados,

7. el algoritmo de cifrado y su parametrización (por ejemplo, longitud de clave, modo de funcionamiento, si procede) se ajustan al estado de la técnica y pueden considerarse sólidos contra el criptoanálisis realizado por las autoridades públicas del país receptor, teniendo en cuenta los recursos y las capacidades técnicas (por ejemplo, la capacidad informática para ataques de fuerza bruta) de que disponen,
8. la fuerza del cifrado tiene en cuenta el período específico durante el cual debe preservarse la confidencialidad de los datos personales cifrados,
9. el algoritmo de cifrado se aplica sin defectos mediante programas informáticos adecuadamente conservados cuya conformidad con la especificación del algoritmo elegido se ha verificado, por ejemplo, mediante una certificación,
10. se ha descartado la existencia de puertas traseras (en el *hardware* o el *software*),
11. el exportador o una entidad en la que confía el exportador en una jurisdicción que ofrece un nivel de protección esencialmente equivalente gestionan (generan, administran, almacenan, si procede, vinculan a la identidad del destinatario previsto y revocan) las claves de forma fiable,

el CEPD considerará que el cifrado de transporte, si es necesario en combinación con el cifrado de contenidos de extremo a extremo, aporta una medida complementaria eficaz.

Caso de uso 4: receptor protegido

85. Un exportador de datos transfiere datos personales a un importador de datos de un tercer país protegido específicamente por el Derecho de ese país, por ejemplo, con el fin de proporcionar conjuntamente tratamiento médico a un paciente o servicios jurídicos a un cliente.

Si

1. el Derecho de un tercer país exime a un importador de datos residente de infringir potencialmente el acceso a los datos en poder de dicho receptor para el fin de que se trate, por ejemplo, en virtud de una obligación de secreto profesional aplicable al importador de datos,
2. esta exención se extiende a toda la información que obra en poder del importador de datos y que puede utilizarse para eludir la protección de información privilegiada (claves criptográficas, contraseñas, otras credenciales, etc.),
3. el importador de datos no emplea los servicios de un encargado del tratamiento de manera que permita a las autoridades públicas acceder a los datos en poder del encargado del tratamiento, ni los transmite a otra entidad que no está protegida, con arreglo a los instrumentos de transferencia del artículo 46 del RGPD,
4. los datos personales se cifran antes de transmitirse con un método acorde con el estado de la técnica que garantiza que el descifrado no será posible sin el conocimiento de la clave de descifrado (cifrado de extremo a extremo) durante todo el período en que es necesario proteger los datos,
5. la clave de descifrado se encuentra bajo la custodia exclusiva del importador de datos protegido y está adecuadamente asegurada contra la utilización o divulgación no autorizadas mediante medidas técnicas y organizativas conformes con el estado de la técnica, y
6. el exportador de datos ha comprobado con fiabilidad que la clave de cifrado que se propone utilizar corresponde a la clave de descifrado que posee el receptor,

el CEPD considerará que el cifrado de transporte efectuado constituye una medida complementaria eficaz.

Caso de uso 5: tratamiento fraccionado o multipartito

86. El exportador de datos desea que los datos personales sean tratados conjuntamente por dos o más encargados independientes situados en diferentes jurisdicciones, sin divulgarles el contenido de los datos. Antes de la transmisión, fracciona los datos de tal manera que ninguna parte recibida por el encargado del tratamiento es suficiente para reconstruir total o parcialmente los datos personales. El exportador de datos recibe el resultado del tratamiento de cada uno de los encargados de forma independiente y une las partes recibidas para llegar al resultado final que puede constituir datos personales o agregados.

Si

1. un exportador de datos trata datos personales de tal manera que se dividen en dos o más partes, cada una de las cuales ya no puede ser interpretada o atribuida a un interesado específico sin el uso de información adicional,
2. cada uno de los elementos se transfiere a un encargado del tratamiento situado en una jurisdicción diferente,
3. opcionalmente, los encargados tratan los datos conjuntamente, por ejemplo utilizando una computación multipartita segura, de forma que no se revela a ninguno de ellos información de la que no disponen antes del cálculo,
4. el algoritmo utilizado para la computación compartida es seguro frente a adversarios activos,
5. no hay pruebas de colaboración entre las autoridades públicas situadas en las jurisdicciones respectivas en las que se encuentra cada uno de los encargados del tratamiento, lo que les permitiría acceder a todos los conjuntos de datos personales que obran en poder de dichos encargados y les permitiría reconstituir y explotar el contenido de los datos personales de forma clara en circunstancias en las que dicha explotación no respetaría el contenido esencial de los derechos y libertades fundamentales de los interesados. Del mismo modo, las autoridades públicas de cualquiera de los dos países no deben estar facultadas para acceder a los datos personales que obran en poder de los encargados del tratamiento en todas las jurisdicciones interesadas,
6. el responsable del tratamiento ha comprobado, mediante un análisis exhaustivo de los datos en cuestión, teniendo en cuenta cualquier información de que dispongan las autoridades públicas de los países destinatarios, que los datos personales que transmite a los encargados del tratamiento no pueden atribuirse a una persona física identificada o identificable, incluso si se realiza una referencia cruzada a dicha información,

el CEPD considerará que el tratamiento fraccionado efectuado constituye una medida complementaria efectiva.

Supuestos en los que no se pueden encontrar medidas *eficaces*

87. Las medidas descritas a continuación en determinados supuestos no serían eficaces para garantizar un nivel de protección esencialmente equivalente para los datos transferidos al tercer país. Por lo tanto, no se considerarían medidas complementarias.

Caso de uso 6: transferencia a proveedores de servicios en la nube u otros encargados del tratamiento que requieran acceso a los datos sin cifrar

88. Un exportador de datos utiliza a un proveedor de servicios en la nube u otro encargado del tratamiento para que los datos personales sean tratados de acuerdo con sus instrucciones en un tercer país.

    Si

    1. un responsable transfiere datos a un proveedor de servicios en la nube u otro encargado del tratamiento,
    2. el proveedor de servicios en la nube u otro encargado del tratamiento necesita acceder a los datos sin cifrar para ejecutar la tarea asignada, y
    3. el poder otorgado a las autoridades públicas del país receptor para acceder a los datos transferidos va más allá de lo necesario y proporcionado en una sociedad democrática,[71]

    el CEPD, teniendo en cuenta el estado actual de la técnica, no podrá plantear una medida técnica eficaz para impedir que dicho acceso vulnere los derechos de los interesados. El CEPD no descarta que los futuros avances tecnológicos puedan posibilitar medidas que logren los fines comerciales previstos, sin necesitar un acceso sin cifrar.

89. En las situaciones descritas, cuando los datos personales no cifrados son técnicamente necesarios para la prestación del servicio por parte del encargado, el cifrado de transporte y el cifrado de datos en reposo, incluso considerados conjuntamente, no constituyen una medida complementaria que garantiza un nivel de protección esencialmente equivalente si el importador de datos está en posesión de las claves criptográficas.

Caso de uso 7: acceso remoto a los datos con fines empresariales

90. Un exportador de datos pone datos personales a disposición de entidades de un tercer país para su uso con fines comerciales compartidos. Una situación típica puede consistir en que un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro transfiera datos personales a un responsable o encargado en un tercer país perteneciente al mismo grupo de empresas o a un grupo de empresas dedicadas a una actividad económica conjunta. Por ejemplo, el importador de datos puede utilizar los datos que recibe para prestar servicios de personal al exportador de datos, para lo que necesita datos de recursos humanos, o para comunicarse con los clientes del exportador de datos residentes en la Unión Europea por teléfono o correo electrónico.

    Si

    1. un exportador de datos transfiere datos personales a un importador de datos de un tercer país poniéndolos a disposición en un sistema de información de uso común de un modo que permite al importador acceder directamente a los datos de su elección, o transfiriéndolos directamente, individualmente o en bloque, mediante el uso de un servicio de comunicación,
    2. el importador utiliza los datos sin cifrar para sus propios fines,
    3. el poder otorgado a las autoridades públicas del país receptor para acceder a los datos transferidos va más allá de lo necesario y proporcionado en una sociedad democrática,

[71] Véanse los artículos 47 y 52 de la Carta de los Derechos Fundamentales de la Unión Europea, el artículo 23, apartado 1, del RGPD y las recomendaciones del CEPD sobre las garantías esenciales europeas para medidas de vigilancia.

el CEPD no podrá plantear una medida técnica eficaz para impedir que dicho acceso vulnere los derechos de los interesados.

91. En las situaciones descritas, cuando los datos personales no cifrados son técnicamente necesarios para la prestación del servicio por parte del encargado, el cifrado de transporte y el cifrado de datos en reposo, incluso considerados conjuntamente, no constituyen una medida complementaria que garantiza un nivel de protección esencialmente equivalente si el importador de datos está en posesión de las claves criptográficas.

Medidas contractuales adicionales

92. Estas medidas consistirán generalmente en compromisos contractuales unilaterales, bilaterales o multilaterales.[72] [73] Si se utiliza un instrumento de transferencia del artículo 46 del RGPD, en la mayoría de los casos ya contendrá una serie de compromisos (principalmente contractuales) por parte del exportador y el importador de datos destinados a servir de garantías de los datos personales.[74]

93. En algunas situaciones, estas medidas pueden complementar y reforzar las garantías que el instrumento de transferencia y el Derecho pertinente del tercer país pueden proporcionar, cuando, teniendo en cuenta las circunstancias de la transferencia, estas no cumplan todas las condiciones necesarias para garantizar un nivel de protección esencialmente equivalente al garantizado en la Unión. Habida cuenta de la naturaleza de las medidas contractuales, que por lo general no pueden vincular a las autoridades de ese tercer país cuando no formen parte del contrato[75], estas deberán combinarse con otras medidas técnicas y organizativas para proporcionar el nivel de protección de datos requerido. Seleccionar y aplicar una o varias de estas medidas no garantizará necesaria y sistemáticamente que su transferencia cumple la norma de equivalencia esencial que exige el Derecho de la Unión.

94. Dependiendo de las medidas contractuales ya incluidas en el instrumento de transferencia del artículo 46 del RGPD que sirve de base, también pueden ser útiles medidas contractuales adicionales para permitir que los exportadores de datos residentes en el EEE tengan conocimiento de nuevos acontecimientos que afecten a la protección de los datos transferidos a terceros países.

95. Como se ha dicho, las medidas contractuales no podrán excluir la aplicación de la legislación de un tercer país que no cumple la norma sobre garantías esenciales europeas del CEPD en aquellos casos en los que la legislación obligue a los importadores a cumplir las órdenes de divulgar los datos que reciban de las autoridades públicas.[76]

---

[72] Por ejemplo, dentro de las NCV que, en cualquier caso, deberán regular algunas de las medidas enumeradas a continuación.

[73] Tendrán carácter privado y no se considerarán acuerdos internacionales con arreglo al Derecho internacional público. En consecuencia, normalmente no vincularán a la autoridad pública del tercer país como parte ajena al contrato cuando se celebre con entidades privadas de terceros países, como subrayó el Tribunal en su sentencia C-311/18 (Schrems II), apartado 125.

[74] Véase la sentencia C-311/18 (Schrems II), apartado 137, en la que el Tribunal reconoció, en consecuencia, que la CPT contiene «*mecanismos efectivos que permit[e]n en la práctica garantizar que el nivel de protección exigido por el Derecho de la Unión sea respetado y que las transferencias de datos personales basadas en esas cláusulas sean suspendidas o prohibidas en caso de violación de dichas cláusulas o de que resulte imposible su cumplimiento*» (véase también el apartado 148).

[75] C-311/18 (Schrems II), apartado 125.

[76] Sentencia del TJUE C-311/18 (Schrems II), apartado 132.

96. A continuación se enumeran algunos ejemplos de estas posibles medidas contractuales, clasificados en función de su naturaleza:

Establecimiento de la obligación contractual de utilizar medidas técnicas específicas

97. ***Dependiendo de las circunstancias específicas de las transferencias, es posible que el contrato tenga que prever que, para que estas se lleven a cabo, deberán aplicarse medidas técnicas específicas (véanse en lo que antecede las medidas técnicas sugeridas).***

98. ***Condiciones para la eficacia:***

- Esta cláusula podría ser eficaz en aquellas situaciones en las que el exportador haya determinado la necesidad de medidas técnicas. En tal caso, tendría que presentarse en una forma jurídica para garantizar que el importador también se compromete a aplicar las medidas técnicas necesarias eventualmente.

Obligaciones de transparencia:

99. ***El exportador podría añadir anexos al contrato con información que el importador proporcionaría, en la medida de sus posibilidades, sobre el acceso a los datos por parte de las autoridades públicas, incluido en el ámbito de la inteligencia, siempre que la legislación cumpla las garantías esenciales europeas del CEPD en el país de destino. Esto podría ayudar al exportador de datos a cumplir su obligación de documentar su evaluación del nivel de protección en el tercer país.***

100. Por ejemplo, podría exigirse al importador:

(1) enumerar las disposiciones legales y reglamentarias del país de destino aplicables al importador o a sus encargados o subencargados del tratamiento que permitan el acceso de las autoridades públicas a los datos personales objeto de la transferencia, en particular en los ámbitos de la inteligencia, la aplicación de las leyes y la supervisión administrativa y reguladora aplicables a los datos transferidos;
(2) en ausencia de leyes que regulen el acceso de las autoridades públicas a los datos, proporcionar información y estadísticas basadas en la experiencia del importador o informes procedentes de diversas fuentes (por ejemplo, socios, fuentes abiertas, jurisprudencia nacional y decisiones de los organismos de supervisión) sobre el acceso de las autoridades públicas a los datos personales en situaciones del tipo de transferencia de datos en cuestión (es decir, en el ámbito normativo específico, en relación con el tipo de entidades a las que pertenece el importador de datos...);
(3) indicar qué medidas se han adoptado para impedir el acceso a los datos transferidos (en su caso);
(4) facilitar información suficientemente detallada sobre todas las solicitudes de acceso a datos personales presentadas por las autoridades públicas que el importador haya recibido durante un período de tiempo determinado,[77] en particular en los ámbitos mencionados en el

[77] La duración del período dependerá del riesgo para los derechos y libertades de los interesados cuyos datos sean objeto de la transferencia en cuestión, por ejemplo, el último año anterior al cierre del instrumento de exportación de datos con el exportador de datos.

apartado 1 anterior, y que incluya información sobre las solicitudes recibidas, los datos solicitados, el organismo solicitante y la base jurídica para la divulgación, así como en qué medida el importador ha divulgado la solicitud de datos;[78]

(5) especificar si, y en qué medida, pesa sobre el importador la prohibición legal de facilitar la información mencionada en los apartados 1 a 5 anteriores.

101. Esta información podría facilitarse a través de cuestionarios estructurados que el importador cumplimentaría y firmaría y se completaría con la obligación contractual del importador de declarar en un plazo determinado cualquier posible cambio en esta información, como es la práctica actual en los procesos de diligencia debida.

102. ***Condiciones para la eficacia:***

- El importador debe ser capaz de facilitar al exportador este tipo de información según su leal saber y entender y después de haber hecho todo lo posible para obtenerla.[79]
- Esta obligación impuesta al importador es un medio para garantizar que el exportador sea siempre consciente de los riesgos asociados a la transferencia de datos a un tercer país. De este modo, permitirá al exportador renunciar a celebrar el contrato o, si la información cambia tras su celebración, cumplir su obligación de suspender la transferencia o rescindir el contrato si el Derecho del tercer país, las garantías contenidas en el instrumento de transferencia del artículo 46 del RGPD utilizado y cualquier otra garantía adicional que pueda haber adoptado ya no pueden garantizar un nivel de protección esencialmente equivalente al de la Unión. Sin embargo, esta obligación no puede justificar la divulgación de datos personales por parte del importador ni dar lugar a la expectativa de que no habrá más solicitudes de acceso.

***

103. ***El exportador también podría añadir cláusulas en virtud de las cuales el importador certificara que: 1) no ha creado deliberadamente puertas traseras o una programación similar que pueda utilizarse para acceder al sistema o a los datos personales; 2) no ha creado o modificado intencionadamente sus procesos comerciales de un modo que facilite el acceso a los datos personales o los sistemas, y 3) el Derecho o la política gubernamental nacionales no exigen que el importador cree o mantenga puertas traseras ni facilite el acceso a los datos personales o los sistemas o que el importador esté en posesión de la clave de cifrado o que la entregue.***[80]

104. ***Condiciones para la eficacia:***

- La existencia de legislación o de políticas gubernamentales que impidan a los importadores divulgar esta información puede hacer ineficaz esta cláusula. Por lo tanto, el importador no podrá celebrar el contrato o tendrá que notificar al exportador su incapacidad para seguir cumpliendo sus compromisos contractuales.[81]

[78] El cumplimiento de esta obligación no equivale, como tal, a proporcionar un nivel de protección adecuado. Al mismo tiempo, cualquier divulgación inadecuada que se haya producido hace necesaria la aplicación de medidas complementarias.

[79] Véase el apartado 32.5 anterior.

[80] Esta cláusula es importante para garantizar un nivel adecuado de protección de los datos personales transferidos y normalmente deberá exigirse.

[81] Véase el apartado 32.5 anterior.

- El contrato deberá incluir sanciones o la capacidad del exportador de rescindir el contrato con un breve preaviso en los casos en los que el importador no revele la existencia de una puerta trasera, de una programación similar o de procesos empresariales manipulados, o la obligación de aplicar alguno de ellos, o bien no informe inmediatamente al exportador una vez que tenga conocimiento de su existencia.

***

105. ***El exportador podría reforzar su facultad de llevar a cabo auditorías[82] o inspecciones de las instalaciones de tratamiento de datos del importador, presenciales o a distancia, para verificar si se han comunicado datos a las autoridades públicas y en qué condiciones (acceso no más allá de lo necesario y proporcionado en una sociedad democrática), por ejemplo, estableciendo un breve preaviso y mecanismos que garanticen la rápida intervención de los organismos de inspección y reforzando la autonomía del exportador en cuanto a la selección de los organismos de inspección.***

106. ***Condiciones para la eficacia:***

- Para que sea plenamente eficaz, el alcance de la auditoría debe abarcar legal y técnicamente cualquier tratamiento por parte de los encargados o subencargados del importador de los datos personales transmitidos en el tercer país.
- Los registros de acceso y otras vías similares deben ser a prueba de manipulaciones, para que los auditores puedan encontrar pruebas de divulgación. Los registros de acceso y otras vías similares también deben distinguir entre accesos debidos a operaciones comerciales ordinarias y accesos debidos a órdenes o solicitudes de acceso.

***

107. ***Cuando se evaluara inicialmente el Derecho y la práctica del tercer país del importador y se considerara que proporcionaba un nivel de protección esencialmente equivalente al previsto en la Unión para los datos transferidos por el exportador, este podría reforzar en cualquier caso la obligación del importador de datos de informar sin demora al exportador de datos de su incapacidad para cumplir los compromisos contractuales y, en consecuencia, el estándar exigido de «nivel de protección de datos esencialmente equivalente».[83]***

108. Esta incapacidad de cumplimiento puede deberse a cambios en el Derecho o las prácticas del tercer país.[84] Las cláusulas podrían establecer plazos y procedimientos específicos y estrictos para la rápida suspensión de la transferencia de datos o la rescisión del contrato y la devolución o supresión por parte del importador de los datos recibidos. El seguimiento de las solicitudes recibidas, su alcance y la

[82] Véase, por ejemplo, la cláusula 5, letra f), de las CPT entre los responsables y los encargados del tratamiento de la Decisión 2010/87/UE; las auditorías también podrían realizarse en el marco de un código de conducta o mediante una certificación.

[83] Cláusula 5, letra a) y letra d), inciso i), de la Decisión 2010/87/UE relativa a las CPT.

[84] Véase el asunto C-311/18 (Schrems II), apartado 139, en el que el Tribunal afirma que «*si bien la misma cláusula 5, letra d), inciso i), permite al destinatario de la transferencia de datos personales, en caso de que exista una legislación que se lo impida, como una prohibición de carácter penal para preservar la confidencialidad de una investigación llevada a cabo por la policía, no notificar al responsable del tratamiento establecido en la Unión una solicitud jurídicamente vinculante de divulgar los datos personales presentada por una autoridad encargada de la aplicación de la ley, el referido destinatario sigue estando obligado, de conformidad con la cláusula 5, letra a), del anexo de la Decisión CPT, a informar al responsable del tratamiento de que no puede cumplir las cláusulas tipo de protección de datos*».

eficacia de las medidas adoptadas para contrarrestarlas debe proporcionar al exportador indicaciones suficientes para ejercer su deber de suspender o poner fin a la transferencia o rescindir el contrato.

109. ***Condiciones para la eficacia:***

- La notificación deberá tener lugar antes de que se conceda el acceso a los datos. De lo contrario, en el momento en que el exportador reciba la notificación, los derechos de la persona ya podrían haberse vulnerado si la solicitud se basa en leyes de ese tercer país que excedan de lo que permite el nivel de protección de datos previsto en el Derecho de la Unión. La notificación podrá seguir sirviendo para prevenir futuras infracciones y permitir al exportador cumplir su obligación de suspender la transferencia de datos personales al tercer país o rescindir el contrato.
- El importador de datos deberá hacer un seguimiento de cualquier evolución jurídica o política que pueda conducir a su incapacidad para cumplir sus obligaciones e informar sin demora al exportador de datos de dichos cambios, a ser posible antes de su aplicación, para que este pueda recuperar los datos del importador de datos.
- Las cláusulas deberán prever un mecanismo rápido por el que el exportador de datos autorice al importador a proteger los datos o a devolverlos rápidamente al exportador de datos o, si esto no fuera posible, a suprimir o cifrar de forma segura los datos sin esperar necesariamente las instrucciones del exportador, si se alcanza un umbral específico acordado entre el exportador y el importador de datos. El importador deberá aplicar este mecanismo desde el inicio de la transferencia de datos y probarlo periódicamente para asegurarse de que puede aplicarse en poco tiempo.
- Otras cláusulas podrían permitir al exportador controlar el cumplimiento de estas obligaciones por parte del importador a través de auditorías, inspecciones y otras medidas de verificación, y aplicarlas con sanciones al importador o la capacidad del exportador para suspender la transferencia o rescindir inmediatamente el contrato.

***

110. ***En la medida en que lo permita el Derecho nacional del tercer país, el contrato podría reforzar las obligaciones de transparencia del importador estableciendo un mecanismo de seguridad, en virtud del cual el importador se comprometería a publicar periódicamente (por ejemplo, cada 24 horas) un mensaje firmado criptográficamente para informar al exportador de que, a partir de una fecha y hora determinadas, no ha recibido ninguna orden de divulgación de datos personales o similares. La ausencia de una actualización de esta notificación indicará al exportador que el importador puede haber recibido una orden.***

111. ***Condiciones para la eficacia:***

- La normativa del tercer país deberá permitir al importador de datos emitir esta forma de notificación pasiva al exportador.
- El exportador de datos deberá supervisar automáticamente las notificaciones del mecanismo de seguridad.
- El importador de datos deberá velar por que su clave privada para la firma del mecanismo de seguridad se mantenga a salvo y asegurar que la normativa del tercer país no le pueda obligar a falsear dicho mecanismo. A tal fin, podría ser útil que fueran necesarias varias firmas de

personas diferentes o que el mecanismo de seguridad fuera gestionado por una persona fuera de la jurisdicción del tercer país.

Obligaciones de tomar medidas específicas

112. ***El importador podría comprometerse a revisar, con arreglo al Derecho del país de destino, la legalidad de cualquier orden de divulgación de datos, en particular si corresponde a los poderes otorgados a la autoridad pública requirente, y a impugnar la orden si, tras una evaluación minuciosa, llega a la conclusión de que existen motivos con arreglo a la legislación del país de destino para hacerlo. Al impugnar una orden, el importador de datos deberá solicitar medidas cautelares para suspender sus efectos hasta que el órgano jurisdiccional se haya pronunciado sobre el fondo del asunto. El importador tendría la obligación de no divulgar los datos personales solicitados hasta que se le exigiera hacerlo con arreglo a las normas de procedimiento aplicables. El importador de datos también se comprometería a facilitar la cantidad mínima de información admisible al responder a la orden, con arreglo a una interpretación razonable de la misma.***

113. ***Condiciones para la eficacia:***

- El ordenamiento jurídico del tercer país deberá ofrecer vías legales efectivas para impugnar órdenes de divulgación de datos.
- Esta cláusula ofrecerá siempre una protección adicional muy limitada, ya que una orden de divulgación de datos puede ser legal con arreglo al ordenamiento jurídico del tercer país, pero este podría no cumplir las normas de la Unión. Esta medida contractual tendrá que ser necesariamente adicional a otras medidas complementarias.
- Los recursos contra las órdenes deben tener un efecto suspensivo con arreglo al Derecho del tercer país. De lo contrario, las autoridades públicas seguirían teniendo acceso a los datos de los interesados y cualquier acción posterior a favor de los mismos tendría el efecto limitado de permitirles reclamar daños y perjuicios por las consecuencias negativas derivadas de la divulgación de los datos.
- El importador tendrá que poder documentar y demostrar al exportador las medidas que ha adoptado, haciendo todo lo posible por cumplir este compromiso.

***

114. ***En la misma situación descrita anteriormente, el importador podría comprometerse a informar a la autoridad pública requirente de la incompatibilidad de la orden con las garantías contenidas en el artículo 46 del RGPD[85] y el consiguiente conflicto de obligaciones para el importador. El importador lo notificaría simultáneamente y lo antes posible al exportador o a la autoridad de control competente del EEE, en la medida de lo posible de conformidad con el ordenamiento jurídico del tercer país.***

[85] Por ejemplo, las CPT establecen que el tratamiento de datos, incluida su transferencia, se ha llevado a cabo y seguirá realizándose de conformidad con «*la legislación de protección de datos aplicable*». Esta ley se define como «*la legislación que protege los derechos y libertades fundamentales de las personas y, en particular, su derecho a la vida privada respecto del tratamiento de los datos personales, aplicable al responsable del tratamiento en el Estado miembro en que está establecido el exportador de datos*». El TJUE confirma que las disposiciones del RGPD, interpretadas a la luz de la Carta de los Derechos Fundamentales de la Unión Europea, forman parte de dicha legislación; véase TJUE C-311/18 (Schrems II), apartado 138.

115. ***Condiciones para la eficacia:***

- Para añadir cierta protección a los datos, dicha información sobre la protección conferida por el Derecho de la Unión y el conflicto de obligaciones deberá tener algún efecto legal en el ordenamiento jurídico del tercer país, como una revisión judicial o administrativa de la orden o la solicitud de acceso, la exigencia de una orden judicial o una suspensión temporal de la orden.
- El ordenamiento jurídico del país no deberá impedir que el importador notifique al exportador o, al menos, a la autoridad de control competente del EEE, la orden o solicitud de acceso recibida.
- El importador tendrá que poder documentar y demostrar al exportador las medidas que ha adoptado, haciendo todo lo posible por cumplir este compromiso.

Facultar a los interesados para que ejerzan sus derechos

116. ***El contrato podría establecer que los datos personales transmitidos en texto sencillo en el curso normal de la actividad comercial (incluidos los casos de asistencia) solo puedan ser consultados con el consentimiento expreso o tácito del exportador o del interesado.***

117. ***Condiciones para la eficacia:***

- Esta cláusula podría ser eficaz en aquellas situaciones en las que los importadores reciben solicitudes de cooperación voluntaria de las autoridades públicas, en contraposición, por ejemplo, al acceso a los datos por parte de las autoridades públicas sin el conocimiento del importador de datos o contra su voluntad.
- En algunas situaciones, el interesado podría no estar en condiciones de oponerse al acceso o de dar un consentimiento que cumpla todas las condiciones establecidas en el Derecho de la Unión (libre, específico, informado e inequívoco) (por ejemplo, en el caso de los empleados)[86].
- Las normativas o políticas nacionales que prohíban al importador divulgar la orden de acceso pueden dejar sin efecto esta cláusula, a menos que pueda respaldarse con métodos técnicos que exijan la intervención del exportador o del interesado para que los datos contenidos en el texto sencillo sean accesibles. Tales medidas técnicas para restringir el acceso pueden contemplarse, en particular, si el acceso solo se concede en casos específicos de asistencia o servicio, pero los propios datos se almacenan en el EEE.

***

118. ***El contrato podría obligar al importador o al exportador a notificar sin demora al interesado la solicitud u orden recibida de las autoridades públicas del tercer país, o la incapacidad del importador para cumplir los compromisos contractuales, a fin de que el interesado pueda solicitar información y obtener un recurso efectivo (por ejemplo, presentando una reclamación ante su autoridad de control o autoridad judicial competente y demostrando su legitimación ante los tribunales del tercer país).***

[86] Artículo 4, apartado 11, del RGPD.

119. ***Condiciones para la eficacia:***

- Esta notificación podría alertar al interesado de posibles accesos a sus datos por parte de las autoridades públicas de terceros países. De este modo, podría permitirle solicitar información adicional a los exportadores y presentar una reclamación ante su autoridad de control competente. Esta cláusula también podría abordar algunas de las dificultades a las que puede enfrentarse una persona a la hora de demostrar su legitimación *(locus standi)* ante órganos jurisdiccionales de terceros países para impugnar el acceso de las autoridades públicas a sus datos.
- Las normativas y políticas nacionales podrían impedir esta notificación al interesado. No obstante, el exportador y el importador podrían comprometerse a informar al interesado tan pronto como se levanten las restricciones a la divulgación de datos y a hacer todo lo posible para obtener la exención de la prohibición de divulgación. Como mínimo, el exportador o la autoridad de control competente podrían notificar al interesado la suspensión o finalización de la transferencia de sus datos personales debido a la incapacidad del importador para cumplir sus compromisos contractuales como consecuencia de la recepción de una solicitud de acceso.

***

120. ***El contrato podría obligar al exportador y al importador a ayudar al interesado en el ejercicio de sus derechos en la jurisdicción del tercer país a través de mecanismos de recurso y asesoramiento jurídico específicos.***

121. ***Condiciones para la eficacia:***

- Las normativas y políticas nacionales podrían imponer condiciones que, a su vez, podrían menoscabar la eficacia de los mecanismos de recurso específicos previstos.
- El asesoramiento jurídico podría ser útil para el interesado, especialmente teniendo en cuenta la complejidad y el coste que puede tener para el mismo comprender el ordenamiento jurídico de un tercer país y ejercer acciones legales desde el extranjero, posiblemente en una lengua distinta a la propia. Sin embargo, esta cláusula ofrecerá siempre una protección adicional limitada, ya que prestar asistencia y asesoramiento jurídico a los interesados no puede por sí solo subsanar la incapacidad de un ordenamiento jurídico de un tercer país para ofrecer un nivel de protección esencialmente equivalente al garantizado en la Unión. Esta medida contractual tendrá que ser necesariamente adicional a otras medidas complementarias.

Esta medida complementaria solo sería eficaz si el Derecho del tercer país prevé vías de recurso ante sus órganos jurisdiccionales nacionales o si existe un mecanismo de recurso específico. En cualquier caso, no se trataría, sin embargo, de una medida complementaria eficaz contra las medidas de vigilancia de no existir un mecanismo de recurso.

Medidas organizativas

122. Las medidas organizativas adicionales pueden consistir en políticas internas, métodos organizativos y normas que los responsables y encargados del tratamiento podrían aplicarse a sí mismos e imponer a los importadores de datos en terceros países. Pueden contribuir a garantizar la coherencia en la protección de los datos personales durante todo el ciclo del tratamiento. Las medidas organizativas también pueden mejorar la concienciación de los exportadores sobre el riesgo y los intentos de acceder a los datos en terceros países, así como sobre su capacidad de reaccionar al respecto. Seleccionar y aplicar una o varias de estas medidas no garantizará necesaria y sistemáticamente que su transferencia cumple la norma de equivalencia esencial que exige el Derecho de la Unión. En función de las circunstancias específicas de la transferencia y de la evaluación realizada sobre el Derecho del tercer país, se necesitarán medidas organizativas para complementar las medidas contractuales o técnicas, a fin de garantizar un nivel de protección de los datos personales esencialmente equivalente al garantizado en la Unión.

123. La evaluación de las medidas más adecuadas deberá realizarse caso por caso, teniendo presente la necesidad de que los responsables y encargados del tratamiento respeten el principio de responsabilidad proactiva. A continuación, el CEPD enumera algunos ejemplos de medidas organizativas que los exportadores pueden aplicar, aunque la lista no es exhaustiva y también puedan resultar adecuadas otras medidas:

Políticas internas de gobernanza de las transferencias, especialmente con grupos de empresas

124. ***Adopción de políticas internas adecuadas con una clara asignación de responsabilidades para las transferencias de datos, canales de denuncia y procedimientos normalizados de trabajo para los casos de solicitudes encubiertas u oficiales de acceso a los datos por parte de las autoridades públicas. Especialmente en el caso de las transferencias entre grupos de empresas, estas políticas pueden incluir, entre otras cosas, el nombramiento de un equipo específico, que deberá tener su domicilio social en el EEE, compuesto de expertos en legislación en materia de TI, protección de datos y privacidad, para tratar las solicitudes relativas a datos personales transferidos desde la Unión; la notificación a la alta dirección jurídica y corporativa y al exportador de datos en el momento de la recepción de dichas solicitudes; las fases de procedimiento para impugnar solicitudes desproporcionadas o ilícitas y el suministro de información transparente a los interesados.***

125. Desarrollo de procedimientos de formación específicos para el personal encargado de gestionar las solicitudes de acceso a los datos personales de las autoridades públicas, que deberán actualizarse periódicamente para reflejar los nuevos avances legislativos y jurisprudenciales en el tercer país y en el EEE. Los procedimientos de formación deberán incluir los requisitos de la legislación de la Unión relativos al acceso de las autoridades públicas a los datos personales, en particular de conformidad con el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales. Deberá aumentarse la sensibilización del personal, en particular mediante la evaluación de ejemplos prácticos de solicitudes de acceso a los datos de las autoridades públicas y aplicando a dichos ejemplos la norma establecida en el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales. Dicha formación deberá tener en cuenta la situación particular del importador de datos, por ejemplo, la legislación y la normativa del tercer país a las que esté sujeto el importador de datos, y deberá desarrollarse en la medida de lo posible en cooperación con el exportador de datos.

126. ***Condiciones para la eficacia:***

- Estas políticas solo pueden contemplarse en aquellos casos en los que la solicitud de las autoridades públicas del tercer país sea compatible con el Derecho de la Unión.[87] Cuando la solicitud sea incompatible, estas políticas no bastarán para garantizar un nivel equivalente de protección de los datos personales y, como ya se ha dicho, deberán interrumpirse las transferencias o adoptarse medidas complementarias adecuadas para evitar el acceso.

Medidas de transparencia y responsabilidad proactiva

127. ***Documentar y registrar las solicitudes de acceso recibidas de las autoridades públicas y la respuesta dada, junto con el razonamiento jurídico y los agentes implicados (por ejemplo, si se ha notificado al exportador y su respuesta, la evaluación del equipo encargado de tramitar tales solicitudes, etc.). Estos registros deben ponerse a disposición del exportador de datos, que, a su vez, debe facilitárselos a los interesados en caso necesario.***

128. ***Condiciones para la eficacia:***

- La legislación nacional del tercer país podría impedir la divulgación de las solicitudes o de información sustancial de las mismas y, por lo tanto, dejar sin efecto esta práctica. El importador de datos deberá informar al exportador de su incapacidad para facilitar tales documentos y registros, ofreciendo así al exportador la posibilidad de suspender las transferencias si dicha incapacidad diera lugar a una disminución del nivel de protección.

***

129. ***Publicación periódica de informes de transparencia o resúmenes relativos a las solicitudes gubernamentales de acceso a los datos y al tipo de respuesta dada, en la medida en que la legislación local permita dicha publicación.***

130. ***Condiciones para la eficacia:***

- La información facilitada debe ser pertinente, clara y lo más detallada posible. La legislación nacional del tercer país podría impedir la divulgación de información detallada. En esos casos, el importador de datos deberá hacer todo lo posible por publicar información estadística o un tipo similar de información agregada.

Métodos de organización y medidas de minimización de datos

131. ***Los requisitos organizativos ya existentes en virtud del principio de responsabilidad proactiva, como la adopción de políticas estrictas y detalladas de acceso a los datos y de confidencialidad y buenas prácticas, basadas en un estricto principio de la necesidad de conocer, supervisadas con auditorías periódicas y aplicadas mediante medidas disciplinarias, también pueden ser medidas útiles en el contexto de una transferencia. A este respecto, deberá considerarse la minimización de datos, a fin de limitar la exposición de los datos personales a accesos no autorizados. Por ejemplo, en algunos casos podría no ser necesario transferir determinados datos (como en el supuesto del acceso remoto***

[87] Véase el asunto C-362/14 («Schrems I»), apartado 94, y el asunto C-311/18 (Schrems II), apartados 168, 174, 175 y 176.

a los datos del EEE, por ejemplo en casos de asistencia, cuando se concede un acceso restringido en lugar de un acceso completo, o cuando la prestación de un servicio solo requiera la transferencia de un conjunto limitado de datos, y no de una base de datos completa).

132. ***Condiciones para la eficacia:***

- Deberán establecerse auditorías periódicas y medidas disciplinarias estrictas para supervisar y hacer cumplir las medidas de minimización de datos también en el contexto de la transferencia.
- El exportador de datos llevará a cabo una evaluación de los datos personales que obren en su poder antes de que tenga lugar la transferencia, a fin de identificar los conjuntos de datos que no son necesarios a efectos de dicha transferencia y que, por tanto, no se compartirán con el importador de datos.
- Las medidas de minimización de datos deberán ir acompañadas de medidas técnicas para garantizar que los datos no estén sujetos a accesos no autorizados. Por ejemplo, la aplicación de mecanismos de computación multipartita segura y la difusión de conjuntos de datos cifrados entre diferentes entidades de confianza pueden impedir, desde el diseño, que cualquier acceso unilateral dé lugar a la divulgación de datos identificables.

***

133. ***Desarrollo de buenas prácticas para implicar de manera adecuada y oportuna y dar acceso a la información al delegado de protección de datos, si existe, y a los servicios jurídicos y de auditoría interna sobre cuestiones relacionadas con las transferencias internacionales de datos personales.***

134. ***Condiciones para la eficacia:***

- El delegado de protección de datos, si existe, y el equipo jurídico y de auditoría interna recibirán toda la información pertinente antes de la transferencia y serán consultados sobre la necesidad de la misma y, en su caso, sobre las garantías adicionales.
- La información pertinente deberá incluir, por ejemplo, la evaluación de la necesidad de la transferencia de los datos personales específicos, una descripción general de la legislación aplicable del tercer país y las garantías que el importador se ha comprometido a aplicar.

Adopción de normas y buenas prácticas

135. ***Adopción de políticas estrictas de seguridad y privacidad de los datos, basadas en la certificación o los códigos de conducta de la Unión o en normas internacionales (por ejemplo, normas ISO), y buenas prácticas (por ejemplo, ENISA), teniendo debidamente en cuenta el estado de la técnica, de acuerdo con el riesgo de las categorías de datos tratados y la probabilidad de que las autoridades públicas intenten acceder a ellos.***

Otros

136. ***Adopción y revisión periódica de políticas internas para evaluar la idoneidad de las medidas complementarias aplicadas e identificar y aplicar soluciones adicionales o alternativas cuando sea necesario, a fin de garantizar que se mantiene un nivel de protección equivalente al garantizado en la Unión a los datos personales transferidos.***

***

137. ***Compromiso del importador de datos de no efectuar ninguna transferencia ulterior de datos personales en el mismo u otro tercer país, o de suspender las transferencias en curso, cuando no pueda garantizarse en el tercer país un nivel de protección de los datos personales equivalente al ofrecido en la Unión.***[88]

[88] C-311/18 (Schrems II), apartados 135 y 137.

ANEXO 3: POSIBLES FUENTES DE INFORMACIÓN PARA EVALUAR UN TERCER PAÍS

138. El importador de datos deberá estar en condiciones de facilitarle las fuentes y la información pertinentes sobre el tercer país en el que está establecido y la legislación aplicable en el mismo. También se podrá remitir a varias fuentes de información, como las enumeradas a continuación de forma no exhaustiva:

- jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) y del Tribunal Europeo de Derechos Humanos (TEDH)[89] a que se refieren las recomendaciones sobre garantías esenciales europeas;[90]
- decisiones de adecuación en el país de destino si la transferencia se fundamenta en una base jurídica diferente;[91]
- resoluciones e informes de organizaciones intergubernamentales, como el Consejo de Europa,[92] otros organismos regionales[93] y organismos y agencias de las Naciones Unidas (por ejemplo, el Consejo de Derechos Humanos[94] y el Comité de Derechos Humanos[95]);
- la jurisprudencia nacional o las decisiones adoptadas por autoridades judiciales o administrativas independientes competentes en materia de confidencialidad y protección de datos de terceros países;
- informes de instituciones académicas y organizaciones de la sociedad civil (por ejemplo, ONG y asociaciones empresariales).

[89] Véase la ficha informativa de la jurisprudencia del TEDH sobre vigilancia masiva: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

[90] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[91] C-311/18 (Schrems II), apartado 141; véanse las decisiones de adecuación en https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[92] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[93] Véanse, por ejemplo, los informes nacionales de la Comisión Interamericana de Derechos Humanos (CIDH), https://www.oas.org/en/iachr/reports/country.asp.

[94] Véase https://www.ohchr.org/SP/HRBodies/UPR/Pages/Documentation.aspx

[95] Véase: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5