



18/ES

WP 254, rev.01

Grupo de trabajo del artículo 29

Referencias sobre adecuación

Aprobado el 28 de noviembre de 2017

Revisado por última vez y aprobado el 6 de febrero de 2018

Este Grupo de Trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un órgano consultivo independiente de la UE en materia de protección de datos e intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

De su secretaría se ocupa la Dirección C (Derechos Fundamentales y Ciudadanía de la Unión) de la Dirección General de Justicia de la Comisión Europea, B-1049, Bruselas, Bélgica, Oficina n.º MO-59 02/013.

Sitio web: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Introducción

El Grupo de Trabajo de las autoridades de protección de datos de UE¹ (el GT29) ha publicado anteriormente un documento de trabajo sobre transferencias de datos personales a terceros países (WP12)². Con la sustitución de la Directiva por el Reglamento general de protección de datos de la UE (RGPD)³, el GT29 está revisando el WP12, sus anteriores directrices, para actualizarlo en el contexto de la nueva legislación y la jurisprudencia reciente del Tribunal de Justicia de la Unión Europea (TJUE)⁴.

El presente documento de trabajo pretende actualizar el capítulo uno del WP12 relativo a la cuestión central del nivel adecuado de protección de los datos en un tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o en una organización internacional (en adelante: «terceros países u organizaciones internacionales»). Este documento será continuamente revisado y, en caso necesario, actualizado durante los próximos años, sobre la base de la experiencia práctica adquirida durante la aplicación del RGPD. Los capítulos 2 (Aplicación del enfoque a países que han ratificado el Convenio 108) y 3 (Aplicación del enfoque a la autorregulación del sector) del WP12 deberán actualizarse más adelante.

El presente documento de trabajo se centra únicamente en las decisiones de adecuación, que son actos de ejecución⁵ de la Comisión Europea, según el artículo 45 del RGPD. Próximos documentos de trabajo que se publicarán de forma independiente (NCV, exenciones) examinarán otros aspectos de las transferencias de datos personales a terceros países y organizaciones internacionales.

Este documento pretende ofrecer orientación a la Comisión Europea y al GT29 en virtud del RGPD para la evaluación del nivel de protección de los datos en terceros países y organizaciones internacionales estableciendo los principios básicos sobre protección de datos que deben estar presentes en el marco jurídico de un tercer país u organización internacional a fin de garantizar una equivalencia esencial con el marco de la UE. Además, puede orientar a terceros países y organizaciones internacionales interesadas en obtener adecuación. No obstante, los principios previstos en este documento de trabajo no se dirigen directamente a los responsables o a los encargados del tratamiento de datos.

El presente documento consta de cuatro capítulos:

Capítulo 1: Información general sobre el concepto de adecuación.

Capítulo 2: Aspectos procedimentales para las decisiones de adecuación en virtud del RGPD.

Capítulo 3: Principios generales en materia de protección de datos. Este capítulo incluye los principios básicos generales en materia de protección de datos para garantizar que el nivel de protección de datos en un tercer país u organización internacional es esencialmente equivalente al establecido por la legislación de la UE.

Capítulo 4: Garantías esenciales para el acceso por parte de los cuerpos policiales y de seguridad nacional a fin de limitar las injerencias en los derechos fundamentales. Este capítulo incluye las garantías esenciales para el acceso por parte de los cuerpos policiales y de seguridad nacional tras la sentencia del asunto Schrems del TJUE en 2015 y sobre la base del documento de trabajo del GT29 sobre garantías esenciales adoptado en 2016.

¹ Como prevé el artículo 29 de la Directiva 95/46/CE sobre protección de datos de la UE.

² Documento de trabajo WP12: Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, adoptado por el Grupo de Trabajo el 24 de julio de 1998.

³ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE).

⁴ Incluido el asunto C-362/14, Maximillian Schrems contra Data Protection Commissioner, 6 de octubre de 2015.

⁵ Véanse el artículo 45, apartado 3, y el artículo 93, apartado 2, del RGPD para saber más sobre los actos de ejecución.

Capítulo 1: Información general sobre el concepto de adecuación

El artículo 45, apartado 1, del RGPD establece el principio de que solo podrá realizarse una transferencia de datos a un tercer país u organización internacional si el tercer país, territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado.

Este concepto de «nivel de protección adecuado», que ya existía en la Directiva 95/46, ha sido ampliado por el TJUE. En este punto, conviene recordar la norma establecida por el TJUE en el asunto Schrems, en particular que, aunque el «nivel de protección» en el tercer país debe ser «sustancialmente equivalente» al garantizado en la UE, «los medios de los que se sirva ese tercer país para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la [UE]»⁶. Por tanto, el objetivo no es reflejar punto por punto la legislación europea, sino establecer los requisitos esenciales y básicos de dicha legislación.

La finalidad de las medidas de adecuación de la Comisión Europea es confirmar formalmente con efectos vinculantes para los Estados miembros⁷ que el nivel de protección de datos en un tercer país u organización internacional es sustancialmente equivalente al nivel de protección de datos en la Unión Europea⁸. Se puede lograr la adecuación a través de una combinación de derechos para los interesados y obligaciones para aquellos que realizan el tratamiento de los datos, o que ejercen control sobre dicho tratamiento, y la supervisión por parte de organismos independientes. No obstante, las normas de protección de datos solo resultan efectivas si son exigibles y se siguen en la práctica. Por tanto, se debe tener en cuenta no solo el contenido de las normas aplicables a los datos personales transferidos a un tercer país u organización internacional, sino también el sistema existente para garantizar la efectividad de dichas normas. Unos mecanismos de aplicación eficientes son de vital importancia para la efectividad de las normas de protección de datos.

El artículo 45, apartado 2, del RGPD establece los elementos que tendrá en cuenta la Comisión Europea a la hora de evaluar la adecuación del nivel de protección en un tercer país u organización internacional.

Por ejemplo, la Comisión tendrá en cuenta el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, la existencia y funcionamiento efectivo de una o más autoridades de control independientes y los compromisos internacionales que haya adoptado el tercer país u organización internacional.

Por tanto, queda claro que cualquier análisis significativo de la protección adecuada debe incluir dos elementos básicos: el contenido de las normas aplicables y los medios para garantizar su aplicación efectiva. Es responsabilidad de la Comisión Europea verificar (de manera periódica) que las normas en vigor son efectivas en la práctica.

El «núcleo» de los principios relativos al «contenido» y los requisitos relativos al «procedimiento/ejecución» de la protección de datos, que se pueden considerar como el requisito mínimo para que la protección sea adecuada, se deriva de la Carta de los Derechos Fundamentales de la Unión Europea y del RGPD. Además, se deben tener en cuenta otros acuerdos internacionales sobre protección de datos, por ejemplo, el Convenio 108⁹.

Asimismo, se debe prestar atención al marco jurídico para el acceso de las autoridades públicas a los datos personales. El documento de trabajo 237 (documento sobre garantías esenciales)¹⁰ ofrece orientaciones adicionales sobre garantías en el contexto de la vigilancia.

⁶ Asunto C-362/14, Maximilian Schrems contra Data Protection Commissioner, 6 de octubre de 2015, apartados 73 y 74.

⁷ Artículo 288, apartado 2, del TFUE.

⁸ Asunto C-362/14, Maximilian Schrems contra Data Protection Commissioner, 6 de octubre de 2015, apartado 52.

⁹ Considerando 105 del RGPD.

¹⁰ Documento de trabajo 01/2016 sobre la justificación de injerencias en los derechos fundamentales a la privacidad y la protección de datos a través de medidas de vigilancia a la hora de transferir datos personales (garantías esenciales europeas), 16/EN WP 237, 13 de abril de 2016.

Las disposiciones generales relativas a la protección de datos y la privacidad en el tercer país no son suficientes. Por el contrario, deben incluirse en el marco jurídico del tercer país u organización internacional disposiciones específicas que aborden necesidades concretas de aspectos prácticos relevantes del derecho a la protección de datos. Estas disposiciones deben tener fuerza ejecutiva.

Capítulo 2: Aspectos procedimentales para las decisiones de adecuación en virtud del RGPD

Para que el Comité Europeo de Protección de Datos cumpla su función de asesorar a la Comisión Europea según el artículo 70, apartado 1, del RGPD, este debe recibir la documentación oportuna, incluida la correspondencia pertinente y las conclusiones de la Comisión Europea. Cuando el marco jurídico sea complejo, se debe incluir cualquier informe elaborado sobre el nivel de protección de datos del tercer país u organización internacional. En cualquier caso, la información ofrecida por la Comisión Europea debe ser exhaustiva y colocar al Comité Europeo de Protección de Datos en una posición que le permita realizar su propia evaluación sobre el nivel de protección de datos en el tercer país. El Comité Europeo de Protección de Datos ofrecerá un dictamen sobre las conclusiones de la Comisión Europea a su debido tiempo y, en caso de existir, identificará insuficiencias en el marco de adecuación. Asimismo, el Comité Europeo de Protección de Datos se esforzará por proponer alternativas o modificaciones para abordar las posibles insuficiencias.

Según el artículo 45, apartado 4, del RGPD es responsabilidad de la Comisión Europea supervisar de manera continuada los acontecimientos que puedan afectar a la efectiva aplicación de las decisiones de adecuación.

El artículo 45, apartado 3, del RGPD prevé realizar una revisión periódica, al menos cada cuatro años. No obstante, este es un plazo general que debe ser ajustado para cada tercer país u organización internacional con una decisión de adecuación. Dependiendo de las circunstancias particulares existentes, se puede justificar un ciclo de revisión más corto. Además, puede que sea necesario llevar a cabo una revisión antes de lo previsto debido a incidentes u otras informaciones sobre el marco jurídico del tercer país u organización internacional en cuestión o a cambios en este. Asimismo, parece adecuado realizar una primera revisión de una decisión completamente nueva lo antes posible y ajustar gradualmente el ciclo de revisión dependiendo del resultado.

Debido al mandato de facilitar a la Comisión Europea un dictamen sobre si el tercer país, territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional ya no pueden garantizar un nivel de protección adecuado, el Comité Europeo de Protección de Datos debe recibir a su debido tiempo información significativa sobre la supervisión de los acontecimientos pertinentes en dicho tercer país u organización internacional por parte de la Comisión Europea. Por tanto, se debe mantener informado al Comité Europeo de Protección de Datos acerca de cualquier proceso o misión de revisión en el tercer país u organización internacional. El Comité Europeo de Protección de Datos apreciará ser invitado a participar en estos procesos y misiones de revisión.

Asimismo, cabe destacar que según el artículo 45, apartado 5, del RGPD, la Comisión tiene derecho a derogar, modificar o suspender decisiones de adecuación existentes. El procedimiento de derogación, modificación o suspensión debe suponer por consiguiente la participación del Comité Europeo de Protección de Datos al solicitarse su dictamen de conformidad con el artículo 70, apartado 1, letra s).

Además, como ya reconoce el artículo 58, apartado 5, del RGPD y según la sentencia del asunto Schrems del TJUE, las autoridades de protección de datos deben tener capacidad para comparecer en juicio si consideran fundada la solicitud de una persona contra una decisión de adecuación: «A ese efecto, corresponde al legislador nacional prever las vías de acción que permitan a la autoridad nacional de control exponer las alegaciones que juzgue fundadas ante los tribunales nacionales, para que éstos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de la Comisión, planteen al Tribunal de Justicia una cuestión prejudicial sobre la validez de ésta¹¹».

¹¹ Asunto C-362/14, Maximillian Schrems contra Data Protection Commissioner, 6 de octubre de 2015, apartado 65.

Capítulo 3: Principios generales en materia de protección de datos para garantizar que el nivel de protección en un tercer país, territorio o uno o varios sectores específicos de ese tercer país, u organización internacional es sustancialmente equivalente al garantizado por la legislación de la UE

El sistema de un tercer país u organización internacional debe incluir los siguientes principios y mecanismos básicos de protección de datos relativos al contenido y al procedimiento/ejecución:

A. Principios relativos al contenido:

1) Conceptos

Deben existir una serie de conceptos o principios básicos sobre protección de datos. Estos no deben imitar la terminología del RGPD, pero deben reflejar los conceptos consagrados en la legislación europea en materia de protección de datos y ser coherentes con ellos. A modo de ejemplo, el RGPD incluye los siguientes conceptos importantes: «datos personales», «tratamiento de datos personales», «responsable del tratamiento», «encargado del tratamiento», «destinatario» y «datos sensibles».

2) Fundamentos del tratamiento lícito y leal para fines legítimos

El tratamiento de los datos debe ser lícito, leal y legítimo.

Las bases legítimas, según las cuales el tratamiento de los datos personales puede ser lícito, leal y legítimo, deben establecerse de manera clara. El marco europeo reconoce varios de estos fundamentos legítimos, incluidas disposiciones en el Derecho nacional, el consentimiento del interesado, la ejecución de un contrato o los intereses legítimos del responsable del tratamiento o de una tercera parte que no prevalezcan sobre los intereses del interesado.

3) Principio de limitación de la finalidad

Los datos deben ser tratados para un fin específico y utilizados posteriormente solo en la medida en que esto no sea incompatible con el fin del tratamiento.

4) Principio de calidad de los datos y proporcionalidad

Los datos deberán ser precisos y, en caso necesario, se mantendrán actualizados. Los datos deberán ser adecuados, pertinentes y no excesivos con respecto a los fines para los que se tratan.

5) Principio de retención de datos

Por regla general, los datos deben almacenarse durante un período no superior al necesario para los fines para los que se tratan.

6) Principio de seguridad y confidencialidad

Cualquier entidad que trate datos personales debe garantizar que estos son tratados de tal manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas. El nivel de seguridad debe tener en cuenta el estado de la técnica y los costes relacionados.

7) Principio de transparencia

Todos las personas deben ser informadas acerca de los elementos principales del tratamiento de sus datos personales en forma clara, de fácil acceso, concisa, transparente e inteligible. Dicha información debe incluir los fines del tratamiento, la identidad del responsable, los derechos a su disposición y otra información en la medida en que esto sea necesario para garantizar la lealtad. En determinadas condiciones, pueden existir ciertas excepciones a este derecho de información como, por ejemplo, salvaguardar investigaciones penales, la seguridad del Estado, la independencia judicial y los procedimientos judiciales u otros objetivos importantes de interés público general como en el caso del artículo 23 del RGPD.

8) Derecho de acceso, rectificación, supresión y oposición

El interesado debe tener derecho a obtener confirmación de si se están tratando o no datos personales que le conciernen, así como derecho de acceso a sus datos personales, incluida una copia de los datos personales objeto de tratamiento.

El interesado debe tener derecho a obtener la rectificación de sus datos según proceda, por razones específicas, por ejemplo, por ser inexactos o incompletos, y a suprimir sus datos personales cuando, por ejemplo, su tratamiento ya no sea necesario o sea ilícito.

Asimismo, el interesado debe tener derecho a oponerse en cualquier momento, por motivos legítimos imperiosos relacionados con su situación particular, al tratamiento de sus datos en condiciones específicas establecidas en el marco jurídico del tercer país. Por ejemplo, en el RGPD estas condiciones incluyen cuando el tratamiento es necesario para la realización de una misión en interés público, cuando es necesario para el ejercicio de poderes públicos conferidos al responsable del tratamiento o cuando el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.

El ejercicio de estos derechos no debe ser excesivamente complicado para el interesado. Pueden existir ciertas restricciones a estos derechos, por ejemplo, salvaguardar investigaciones penales, la seguridad del Estado, la independencia judicial y los procedimientos judiciales u otros objetivos importantes de interés público general como en el caso del artículo 23 del RGPD.

9) Restricciones a transferencias ulteriores

Las transferencias ulteriores de datos personales por parte del destinatario inicial de la transferencia de datos original solo se permitirán cuando otro destinatario (el destinatario de la transferencia ulterior) también esté sujeto a normas (incluidas normas contractuales) que otorguen un nivel de protección adecuado y cumplan las instrucciones pertinentes al tratar los datos en nombre del responsable del tratamiento. El nivel de protección de las personas físicas cuyos datos se transfieran no debe verse menoscabado por la transferencia ulterior. El destinatario inicial de los datos transferidos desde la UE será responsable de garantizar que se ofrecen garantías adecuadas para las transferencias ulteriores de datos en ausencia de una decisión de adecuación. Estas transferencias ulteriores de datos solo se deben realizar para unos fines limitados y específicos, y siempre que existan fundamentos jurídicos para dicho tratamiento.

B. Ejemplos de principios de contenido adicionales que deben aplicarse a tipos específicos de tratamiento

1) Categorías especiales de datos

Deben existir salvaguardas específicas cuando se trate de categorías especiales de datos¹². Estas categorías deben reflejar las consagradas en los artículos 9 y 10 del RGPD. Esta protección debe aplicarse mediante requisitos más exigentes para el tratamiento de datos como, por ejemplo, que el interesado dé su consentimiento explícito para el tratamiento, o mediante medidas de seguridad adicionales.

2) Mercadotecnia directa

Cuando los datos sean tratados con fines de mercadotecnia directa, el interesado debe poder oponerse sin coste alguno a que sus datos sean tratados para dichos fines en cualquier momento.

3) Decisiones automatizadas y elaboración de perfiles

Las decisiones basadas únicamente en el tratamiento automatizado (decisiones individuales automatizadas), incluida la elaboración de perfiles, que producen efectos legales o que afectan considerablemente al interesado, solo se pueden adoptar en determinadas condiciones establecidas en el marco jurídico del tercer país. En el marco europeo, estas condiciones incluyen, por ejemplo, la necesidad de obtener el consentimiento explícito del interesado o la necesidad de dicha decisión para la celebración de un contrato. Si la decisión no cumple las condiciones previstas por el marco jurídico del tercer país, el interesado tendrá derecho a no estar sujeto a ella. En cualquier caso, la legislación del tercer país debe ofrecer las garantías necesarias, incluido el derecho a ser informado sobre las razones específicas que sustentan la decisión y la lógica aplicada, a corregir información inexacta o incompleta, y a impugnar la decisión cuando esta haya sido adoptada sobre unos hechos incorrectos.

C. Mecanismos relativos al procedimiento y la ejecución:

Aunque los medios a los que recurra el tercer país para el objetivo de garantizar un nivel de protección adecuado puedan diferir de los empleados en la Unión Europea¹³, un sistema coherente con el europeo debe caracterizarse por la existencia de los siguientes elementos:

1) Autoridades de control competentes independientes

Deben existir una o más autoridades de control independientes, encargadas de supervisar, garantizar y hacer cumplir las disposiciones de protección de datos y privacidad en el tercer país. La autoridad de control deberá actuar con completa independencia e imparcialidad al desempeñar sus obligaciones y ejercer sus poderes y, al hacerlo, no solicitará ni aceptará instrucciones. En dicho contexto, la autoridad de control dispondrá de todos los poderes y misiones necesarios y disponibles para garantizar el cumplimiento de los derechos de protección de datos y fomentar la sensibilización. Asimismo, se debe tener en cuenta el personal y presupuesto de la autoridad de control. Esta también podrá llevar a cabo investigaciones por iniciativa propia.

2) El sistema de protección de datos debe garantizar un buen nivel de cumplimiento

El sistema del tercer país debe garantizar un elevado grado de responsabilidad proactiva y sensibilización entre los responsables del tratamiento y aquellos que llevan a cabo el tratamiento de datos personales en su nombre respecto a sus obligaciones, tareas y responsabilidades, y entre los interesados respecto a sus derechos y los medios para ejercerlos. La existencia de sanciones

¹² Estas categorías especiales son conocidas como «datos sensibles» en el considerando 10 del RGPD.

¹³ Asunto C-362/14, Maximillian Schrems contra Data Protection Commissioner, 6 de octubre de 2015, apartado 74.

efectivas y disuasorias puede desempeñar un papel importante a la hora de asegurar el respeto de las normas, como, por supuesto, lo pueden hacer los sistemas de verificación directa por parte de autoridades, auditores y responsables independientes de la protección de datos.

3) Responsabilidad proactiva

El marco de protección de datos de un tercer país debe obligar a los encargados del tratamiento o a aquellos que realizan el tratamiento de datos en su nombre a cumplirlo y a poder demostrar dicho cumplimiento en particular ante la autoridad de control competente. Estas medidas pueden incluir, por ejemplo, evaluaciones de impacto relativas a la protección de datos, la llevanza de registros de actividades de tratamiento de datos durante un tiempo adecuado, la designación de un delegado de protección de datos o la protección de datos desde el diseño y por defecto.

4) El sistema de protección de datos debe ofrecer apoyo y ayuda a los interesados individuales en el ejercicio de sus derechos y mecanismos de reclamación adecuados

Una persona debe poder interponer un recurso judicial para hacer valer sus derechos de forma rápida y efectiva, y sin costes prohibitivos, así como para garantizar su cumplimiento. Para tal fin, deben aplicarse mecanismos de supervisión que permitan la investigación independiente de reclamaciones y que posibiliten que las infracciones del derecho a la protección de datos y respeto por la vida privada sean identificadas y castigadas en la práctica.

Cuando no se cumplan las normas, también se ofrecerán al interesado mecanismos efectivos de reclamación administrativa y judicial, incluida la indemnización por daños como resultado del tratamiento ilícito de sus datos personales. Este es un elemento básico que debe contemplar un sistema de adjudicación o arbitraje independiente que permita pagar indemnizaciones e imponer sanciones cuando proceda.

Capítulo 4: Garantías esenciales en terceros países para el acceso a los datos por parte de los cuerpos policiales y de seguridad nacional a fin de limitar las injerencias en los derechos fundamentales

Al evaluar la adecuación del nivel de protección, en virtud del artículo 45, apartado 2, letra a), la Comisión debe tener en cuenta «la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación».

La sentencia del asunto Schrems del TJUE señala que «la expresión “nivel de protección adecuado” debe entenderse en el sentido de que exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta». Aunque los medios de los que se sirva ese país tercero para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la Unión, deben ser eficaces en la práctica¹⁴.

En este contexto, el Tribunal también criticó que la anterior Decisión sobre puerto seguro no contenía «ninguna constatación sobre la existencia en Estados Unidos de reglas estatales destinadas a limitar las posibles injerencias en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión a Estados Unidos, injerencias que estuvieran autorizadas a llevar a cabo entidades estatales de ese país cuando persigan fines legítimos, como la seguridad nacional».

El GT29 ha identificado en el dictamen WP237, adoptado el 13 de 2016, garantías esenciales que reflejan la jurisprudencia del TJUE y el CEDH en el ámbito de la vigilancia. Aunque las recomendaciones incluidas en el documento WP237 siguen siendo válidas y deben tenerse en cuenta al evaluar la adecuación de un tercer país en el ámbito de la vigilancia, la aplicación de estas garantías puede diferir en los ámbitos del acceso a los datos por parte de los cuerpos policiales y de seguridad nacional. En todo caso, para ser consideradas adecuadas, los terceros países deben respetar estas cuatro garantías para acceder a los datos, tanto para fines de seguridad nacional como para fines de cumplimiento de la ley.

- 1) El tratamiento debe basarse en normas claras, precisas y accesibles (base jurídica)**
- 2) Se deben demostrar la necesidad y la proporcionalidad respecto a los objetivos legítimos perseguidos**
- 3) El tratamiento debe estar sujeto a una supervisión independiente**
- 4) Las personas deben disponer de vías de acción efectivas**

¹⁴ Asunto C-362/14, Maximillian Schrems contra Data Protection Commissioner, 6 de octubre de 2015, apartado 74.