Recomendaciones

Recomendaciones 01/2021 relativas a las referencias sobre adecuación en el marco de la Directiva sobre protección de datos en el ámbito penal

Adoptadas el 2 de febrero de 2021

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

Historial de versiones

Versión 1.1	6 de julio de 2021	Cambio de formato
Versión 1.0	2 de febrero de 2021	Adopción de las recomendaciones

Índice

El Comité Europeo de Protección de Datos

Visto el artículo 51, apartado 1, letra b), de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo[1],

Vistos los artículos 12 y 22 de su Reglamento interno,

HA ADOPTADO LAS PRESENTES RECOMENDACIONES:

1. INTRODUCCIÓN

1. El Grupo de Trabajo del Artículo 29 (GT29) ha publicado un documento de trabajo[2] relativo a las referencias sobre adecuación con arreglo al Reglamento general de protección de datos (RGPD)[3]. Este documento de trabajo fue aprobado por el Comité Europeo de Protección de Datos (CEPD) en su primera sesión plenaria.

2. Como se indica en la Declaración n.º 21 aneja al Tratado de Lisboa, podrían requerirse normas específicas para la protección de datos de carácter personal y la libre circulación de dichos datos en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial que se basen en el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE), en razón de la naturaleza específica de dichos ámbitos.

3. Sobre esta base, el legislador de la UE aprobó la Directiva (UE) 2016/680 (Directiva sobre protección de datos en el ámbito penal, en adelante «la Directiva») que establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes, con fines de **prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública**.

4. Esta Directiva determina los motivos por los que se permite la transferencia de datos personales a un tercer país o a una organización internacional en este contexto. Uno de los motivos para dicha transferencia es la decisión de la Comisión Europea de que el tercer país u organización internacional en cuestión garantizan un nivel de protección adecuado.

[1] DO L 119 de 4.5.2016, p. 89.
[2] WP254.rev01 adoptado por el GT29 el 28 de noviembre de 2017, revisado por última vez y adoptado el 6 de febrero de 2018. Actualiza el capítulo I del documento de trabajo «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE» (WP12), adoptado por el GT29 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), DO L 119 de 4.5.2016, p. 1.

5. Mientras que el documento de trabajo WP254.rev01 relativo a las referencias sobre adecuación pretende ofrecer orientación a la Comisión Europea sobre el nivel de protección de los datos en terceros países y organizaciones internacionales en virtud del RGPD, el presente documento tiene como objetivo proporcionar una orientación similar en virtud de la Directiva. En este contexto, establece los principios básicos de la protección de datos que deben estar presentes en el marco jurídico de un tercer país o de una organización internacional a fin de garantizar una equivalencia esencial con el marco de la UE dentro del ámbito de aplicación de la Directiva (es decir, para el tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales). Además, puede orientar a terceros países y organizaciones internacionales interesados en obtener adecuación.

6. El presente documento se centra únicamente en las decisiones de adecuación, que son actos de ejecución de la Comisión Europea de acuerdo con el artículo 36, apartado 3, de la Directiva sobre protección de datos en el ámbito penal.

2. CONCEPTO DE ADECUACIÓN

7. La Directiva sobre protección de datos en el ámbito penal establece las normas para la transferencia de datos personales a terceros países y organizaciones internacionales en la medida en que dichas transferencias entren en su ámbito de aplicación. Las normas relativas a las transferencias internacionales de datos personales se establecen en el capítulo V de la Directiva, en particular en sus artículos 35 a 39.

8. De conformidad con el artículo 36 de la Directiva, puede realizarse una transferencia de datos personales 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. Se desprende de la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE)[4] que esta disposición, debe leerse a la luz del artículo 35 de la Directiva, titulado «Principios generales de las transferencias de datos personales», que establece que «todas las disposiciones [del capítulo V de la Directiva] se aplicarán a fin de garantizar que no se menoscabe el nivel de protección de las personas físicas que garantiza esta Directiva».

9. Cuando la Comisión Europea haya decidido que dicho nivel de protección está garantizado, podrán realizarse las transferencias de datos personales a ese tercer país, territorio, sector u organización internacional, sin necesidad de obtener ninguna autorización específica, excepto cuando otro Estado miembro del que se obtuvieron los datos tenga que dar su autorización a la transferencia, tal y como se establece en los artículos 35 y 36 y en el considerando 66 de la Directiva. Esto se entiende sin perjuicio de la necesidad de que las autoridades de los Estados miembros afectados traten los datos de conformidad con las disposiciones nacionales adoptadas en virtud de la Directiva (UE) 2016/680.

[4] Asunto C-311/18, Data Protection Commissioner/Facebook Ireland Limited y Maximillian Schrems, 16 de julio de 2020, ECLI:EU:C:2020:559, apartado 92 (Schrems II).

10. Este concepto de «nivel de protección adecuado», que ya existía en la Directiva 95/46/CE[5] y en la Decisión Marco 2008/977/JAI del Consejo[6], ha sido desarrollado por el TJUE en este contexto y, recientemente, en el marco del RGPD.

11. Tal y como especifica el TJUE, si bien 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 Unión», pero dichos medios «deben ser eficaces en la práctica»[7]. Por tanto, el objetivo del requisito de adecuación no es reflejar punto por punto la legislación europea, sino establecer los requisitos esenciales y básicos de dicha legislación.

12. En este contexto, el Tribunal también aclaró que una decisión de adecuación de la Comisión debe contener alguna constatación sobre la existencia en el tercer país de reglas estatales destinadas a limitar las posibles injerencias en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión Europea a dicho tercer país, injerencias que estuvieran *autorizadas* a llevar a cabo entidades estatales de ese país cuando persigan fines legítimos, como la seguridad nacional[8].

13. La finalidad de las decisiones de adecuación de la Comisión Europea es confirmar formalmente con efectos vinculantes para los Estados miembros[9], también para sus autoridades competentes de protección de datos[10], que el nivel de protección de datos existente en un tercer país u organización internacional es sustancialmente equivalente al nivel de protección de datos en la Unión Europea. El tercer país en cuestión debe ofrecer garantías que aseguren un nivel de protección adecuado que sea esencialmente equivalente al garantizado en la Unión, en particular cuando los datos se sometan a tratamiento en uno o varios sectores específicos[11].

14. 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[12].

---

[5] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281 de 23.11.1995, p. 31.

[6] Decisión Marco 2008/977/JAI, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, DO L 350 de 30.12.2008, p. 60.

[7] Asunto C−362/14, Maximillian Schrems/Data Protection Commissioner, 6 de octubre de 2015, ECLI:EU:C:2015:650, apartados 73 y 74 (Schrems I).

[8] Schrems I, apartado 88.

[9] Artículo 288 del TFUE.

[10] Schrems I, apartado 52.

[11] Considerando 67 de la Directiva sobre protección de datos en el ámbito penal.

[12] Schrems I, apartados 72 a 74 y Dictamen 1/15 del TJUE, sobre el proyecto de acuerdo entre Canadá y la Unión Europea, 26 de julio de 2017, ECLI:EU:C:2017:592 (Dictamen 1/15), apartado 134: «Este derecho a la protección de los datos de carácter personal exige, en concreto, que en caso de transferencia de tales datos desde la Unión a un país tercero, quede garantizada la continuidad del elevado nivel de protección de los derechos y libertades fundamentales conferido por el Derecho de la Unión. Aunque los medios encaminados a garantizar tal nivel de protección puedan ser diferentes de los aplicados en la Unión para garantizar el cumplimiento de las exigencias derivadas del Derecho de la Unión, tales medios deben ser eficaces en la práctica para asegurar una protección sustancialmente equivalente a la garantizada en la Unión».

3. ASPECTOS PROCEDIMENTALES PARA LAS DECISIONES DE ADECUACIÓN EN VIRTUD DE LA DIRECTIVA SOBRE PROTECCIÓN DE DATOS EN EL ÁMBITO PENAL

15. Para que el Comité Europeo de Protección de Datos (CEPD) cumpla su función de asesorar a la Comisión Europea según el artículo 51, apartado 1, letra g) de la Directiva, este debe recibir la documentación oportuna, incluida la correspondencia pertinente y las conclusiones de la Comisión Europea. Es absolutamente necesario que todos los documentos pertinentes se transmitan al CEPD con suficiente antelación y se traduzcan al inglés para permitir debates informados y útiles antes de la adopción final de las decisiones de adecuación. 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 CEPD en una posición que le permita evaluar el análisis llevado a cabo por la Comisión Europea sobre el nivel de protección de datos en el tercer país u organización internacional.

16. El CEPD 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 y ofrecerá posibles recomendaciones, cuando proceda.

17. Según el artículo 36, apartado 4, de la Directiva es responsabilidad de la Comisión Europea supervisar de manera continuada los acontecimientos que puedan afectar al funcionamiento de las decisiones de adecuación.

18. El artículo 36, apartado 3, de la Directiva 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.

19. 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 CEPD 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 CEPD acerca de cualquier proceso o misión de revisión en el tercer país u organización internacional. El CEPD recomienda que se le invite a participar en estos procesos y misiones de revisión, tal como estaba previsto en la decisión sobre el Escudo de la privacidad y está previsto en la decisión de adecuación relativa a Japón.

20. También hay que tener en cuenta que, según el artículo 36, apartado 5, de la Directiva, la Comisión Europea está facultada para derogar, modificar o suspender las decisiones de adecuación existentes cuando el tercer país u organización internacional haya dejado de garantizar un nivel de protección adecuado El procedimiento para derogar, modificar o suspender implica al CEPD, al solicitar su dictamen de conformidad con el artículo 51, apartado 1, letra g), de la Directiva.

21. Asimismo, sin perjuicio de las atribuciones del ministerio fiscal, las autoridades de control deben tener también competencia para poner en conocimiento de las autoridades judiciales las infracciones de dicha Directiva o capacidad para litigar[13]. De la sentencia Schrems I del TJUE se deriva, en particular, que las autoridades de protección de datos deben tener capacidad para comparecer en juicio ante los órganos jurisdiccionales nacionales si consideran fundadas las alegaciones expuestas por una persona contra una decisión de adecuación[14]. La sentencia en el asunto Schrems II confirmó esta apreciación[15].

4. NORMAS DE LA UE PARA LA ADECUACIÓN DE LA COOPERACIÓN POLICIAL Y JUDICIAL EN MATERIA PENAL

22. En cuanto al fondo, las decisiones de adecuación deben centrarse en la evaluación de la legislación vigente del tercer país en cuestión en su conjunto, en la teoría y en la práctica, a la luz de los criterios de evaluación establecidos en el artículo 36 de la Directiva. El sistema de un tercer país u organización internacional debe incluir los siguientes principios y mecanismos básicos de protección de datos de carácter general, de procedimiento y de ejecución:

23. El artículo 36, apartado 2, de la Directiva 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.

24. En particular, la Comisión tendrá en cuenta el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales[16], la legislación pertinente, así como la aplicación de dicha legislación, los derechos efectivos y exigibles de los interesados y un derecho de recurso administrativo y judicial de los interesados cuyos datos personales son transferidos, la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes, así como los compromisos internacionales asumidos por el tercer país u organización internacional.

25. 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

[13] Véanse el artículo 47, apartado 5, de la Directiva y su considerando 82.
[14] Véase Schrems I, apartado 65: «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 ésta».
[15] Véase Schrems II, apartado 120: «[I]ncluso habiendo adoptado la Comisión una decisión de adecuación, la autoridad nacional de control competente, a la que una persona haya presentado una reclamación para proteger sus derechos y libertades frente al tratamiento de datos personales que la conciernen, debe poder apreciar con toda independencia si la transferencia de esos datos cumple las exigencias establecidas por el RGPD y, en su caso, interponer un recurso ante los tribunales nacionales, para que estos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de adecuación, planteen al Tribunal de Justicia una cuestión prejudicial sobre esta validez».
[16] Al evaluar el marco jurídico del tercer país, debe tenerse en cuenta la posibilidad de que se imponga la pena de muerte o cualquier forma de trato cruel e inhumano sobre la base de los datos transferidos desde la UE. De hecho, en caso de que dicha pena o trato esté previsto en la legislación del tercer país, deberán encontrarse salvaguardias adicionales en el marco jurídico del tercer país para garantizar que los datos transferidos desde la UE no se utilicen para solicitar, dictar o ejecutar una pena de muerte o cualquier forma de trato cruel e inhumano (por ejemplo, un acuerdo internacional que imponga condiciones a la transferencia, un compromiso por parte del tercer país de no imponer la pena de muerte o cualquier forma de trato cruel e inhumano sobre la base de los datos transferidos desde la UE o una moratoria de la pena de muerte).

aplicación efectiva en la práctica. Es responsabilidad de la Comisión Europea verificar (de manera periódica) que las normas en vigor son efectivas en la práctica.

26. El núcleo de los principios generales y los requisitos relativos al procedimiento y 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 (en adelante, «la Carta») y del RGPD. 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 en concreto el derecho a la protección de los datos en el ámbito de la aplicación de la ley. El tercer país debe ofrecer garantías que aseguren un nivel de protección adecuado que sea esencialmente equivalente al garantizado en la Unión. Estas disposiciones deben tener fuerza ejecutiva.

27. Por otra parte, en relación con el principio de proporcionalidad[17], el TJUE ha declarado, en relación con la legislación de los Estados miembros, que la cuestión de si se justifica una limitación de los derechos a la intimidad y a la protección de datos debe apreciarse, por una parte, determinando la **gravedad de la injerencia** que supone esa limitación[18] y, por otra parte, comprobando que la **importancia del objetivo de interés general** perseguido por dicha limitación guarde relación con tal gravedad[19].

28. Según la jurisprudencia del TJUE, una base legal que permita injerencias en los derechos fundamentales, para cumplir el principio de proporcionalidad, debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate[20]. Las excepciones a la protección de datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario[21]. A fin de cumplir este requisito, la normativa además de establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión, debe imponer unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. «En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado»[22].

29. El CEPD ha adoptado recomendaciones que indican las garantías esenciales que reflejan la jurisprudencia del TJUE y del Tribunal Europeo de Derechos Humanos (TEDH) en el ámbito de la vigilancia que deben encontrarse en la legislación del tercer país al evaluar las injerencias de dichas medidas de vigilancia con los derechos de los interesados en caso de que los datos se transfieran a ese tercer país en virtud del RGPD[23]. Para evaluar si se cumplen las condiciones del artículo 36, apartado 2, letra a), de la Directiva sobre protección de datos en el ámbito penal, el

[17] Artículo 52, apartado 1, de la Carta.
[18] El tribunal señaló, por ejemplo, que «la injerencia que supone la recopilación en tiempo real de los datos que permiten localizar un equipo terminal parece especialmente grave, pues estos datos facilitan a las autoridades nacionales competentes un método de seguimiento preciso y continuo de los desplazamientos de los usuarios de los teléfonos móviles [...]» (asuntos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, 6 de octubre de 2020, ECLI:EU:C:2020:791, apartado 187, incluida la jurisprudencia citada).
[19] La Quadrature du Net y otros, apartado 131.
[20] Schrems II, apartado 180.
[21] Schrems II, apartado 176, incluida la jurisprudencia citada.
[22] Schrems II, apartado 176, incluida la jurisprudencia citada.
[23] Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia, adoptadas el 10 de noviembre de 2020.

CEPD considera que hay que tener en cuenta las garantías establecidas en estas Recomendaciones a la hora de evaluar la adecuación de un tercer país en virtud de dicha Directiva en el ámbito de la vigilancia, teniendo en cuenta otras condiciones específicas en dicho ámbito en este contexto.

30. En relación con el requisito del artículo 36, apartado 2, letra b), el tercer país no solo debe garantizar la supervisión eficaz e independiente de la protección de datos, sino también establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros[24].

31. En relación con el requisito contemplado en el artículo 36, apartado 2, letra c), además de los compromisos internacionales asumidos por el tercer país o la organización internacional, también deben tenerse en cuenta las obligaciones que deriven de la participación de estos en sistemas multilaterales o regionales, en particular en relación con la protección de datos personales, y el cumplimiento de las citadas obligaciones, en particular la adhesión del tercer país a otros acuerdos internacionales sobre protección de datos, por ejemplo, debe tenerse en cuenta el Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos personales y su Protocolo adicional (Convenio 108[25] y su versión actualizada, Convenio 108+). También se puede tener en cuenta el cumplimiento por parte del tercer país de los principios consagrados en documentos internacionales como la Guía práctica sobre el uso de datos de carácter personal en el sector policial del Consejo de Europa sobre cómo proteger los datos personales al mismo tiempo que se lucha contra la delincuencia.

32. Una decisión de adecuación debe garantizar que, mediante el contenido de los derechos de privacidad y protección de datos y su aplicación, supervisión y cumplimiento efectivos, el sistema extranjero en su conjunto ofrece el nivel de protección requerido, incluso para los datos en tránsito hacia este tercer país. Tal y como subrayó el TJUE en la sentencia Schrems II, el alto nivel de protección ofrecido debe garantizarse también cuando se produzca una transferencia de datos personales a un país tercero[26].

33. Por último, en la adopción de una decisión de adecuación con respecto a un territorio o un sector específico de un tercer país, la Comisión Europea debe tener en cuenta criterios claros y objetivos, como las actividades de tratamiento concretas y el alcance de las normas jurídicas aplicables y la legislación vigente en el tercer país[27].

A. Principios generales y garantías

a) Conceptos

34. Deben existir conceptos básicos sobre protección de datos. Estos no deben imitar la terminología de la Directiva sobre protección de datos en el ámbito penal, 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, la Directiva incluye los siguientes conceptos importantes: «datos personales», «tratamiento de datos personales», «autoridades competentes», «responsable del tratamiento», «encargado del tratamiento», «destinatario», «datos sensibles», «exactitud»,

[24] Considerando 67 de la Directiva sobre protección de datos en el ámbito penal.
[25] Considerando 68 de la Directiva sobre protección de datos en el ámbito penal.
[26] Véase el apartado 93.
[27] Considerando 67 de la Directiva sobre protección de datos en el ámbito penal.

«elaboración de perfiles», «protección de datos desde el diseño y por defecto», «autoridad de control» y «seudonimización».

b) Tratamiento de datos personales lícito y leal (Artículo 4 y Considerando 26)

35. De acuerdo con el artículo 8, apartado 2, de la Carta, los datos de carácter personal se tratarán, entre otras cosas, «para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley»[28]. Sin embargo, en el marco de la aplicación de las leyes, cabe señalar que el ejercicio de las funciones de prevención, investigación, detección o enjuiciamiento de infracciones penales que la legislación atribuye institucionalmente a las autoridades competentes permite a estas exigir u ordenar a las personas físicas que atiendan a las solicitudes que se les dirijan. En este caso, el consentimiento del interesado no constituye un fundamento jurídico para el tratamiento de los datos personales por las autoridades competentes[29].

36. Esta base legal debe establecer reglas claras y precisas que regulen el alcance y la aplicación de las actividades de tratamiento de datos pertinentes e impongan unas exigencias mínimas[30]. Además, el TJUE recordó que «[d]icha normativa debe ser legalmente imperativa en Derecho interno»[31].

37. Para que sea lícito, el tratamiento de datos personales[32] debe ser necesario para el desempeño de una función de interés público llevada a cabo por una autoridad competente con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública[33]. Estos fines deben estar previstos en la legislación nacional.

38. Los datos personales se tratarán de forma leal. El principio de tratamiento leal es un concepto distinto del derecho a un «juicio imparcial», según se define en el artículo 47 de la Carta y en el artículo 6 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH)[34].

c) El principio de limitación de la finalidad (Artículo 4)

[28] Véase Schrems II, apartado 173.

[29] El considerando 35 de la Directiva también establece que «[c]uando se exige al interesado que cumpla una obligación jurídica, este no goza de verdadera libertad de elección, por lo que no puede considerarse que su respuesta constituya una manifestación libre de su voluntad. Ello no debe ser óbice para que los Estados miembros establezcan en su legislación la posibilidad de que el interesado pueda aceptar el tratamiento de sus datos personales a los efectos de la presente Directiva, por ejemplo, para la realización de pruebas de ADN en las investigaciones penales o el control del paradero del interesado mediante dispositivos electrónicos para la ejecución de sanciones penales».

[30] Véase Schrems II, apartados 175 y 180 y el Dictamen 1/15, apartado 139 y la jurisprudencia citada.

[31] Véase el asunto C-623/17, Privacy International/Secretary of State for Foreign and Commonwealth Affairs y otros, 6 de octubre de 2020, ECLI:EU:C:2020:790, apartado 68. También debe quedar claro que en la versión francesa de la sentencia, el TJUE utiliza el término *réglementation*, que no solo abarca los actos del Parlamento.

[32] Tratamiento total o parcialmente automatizado de datos personales, y tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

[33] Se entiende por autoridades competentes toda autoridad pública competente a estos efectos o cualquier otro organismo o entidad a la que la ley encomiende el ejercicio de la autoridad pública y de los poderes públicos a estos efectos.

[34] Considerando 26 de la Directiva sobre protección de datos en el ámbito penal.

39. Los fines específicos a los que obedezca el tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de la recopilación de los datos personales[35].

40. Los datos deben tratarse con fines determinados, explícitos y legítimos, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales[36], incluidas la protección y la prevención frente a las amenazas contra la seguridad pública en el país tercero, y deben utilizarse posteriormente para cualquiera de estos fines en la medida en que no sean incompatibles con la finalidad original del tratamiento (por ejemplo, para procedimientos paralelos de aplicación de la ley o para el archivo en el interés público, el uso científico, estadístico o histórico para dichos fines) y con sujeción a las salvaguardias adecuadas para los derechos y libertades de los interesados. Si el mismo u otro responsable del tratamiento (autoridad competente[37]) trata datos personales con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales distintos de los fines para los que los datos fueron recopilados, dicho tratamiento debe permitirse con la condición de que esté autorizado con arreglo a la legislación aplicable y sea necesario y proporcionado para dicho otro fin[38]. También debe tenerse en cuenta la existencia de un mecanismo para informar a las autoridades competentes de los Estados miembros pertinentes de dicho tratamiento de datos ulterior[39]. Además, en cualquier caso, el nivel de protección de las personas físicas previsto en la Unión por la Directiva no debe verse menoscabado, incluso en aquellos casos en los que los datos personales se transmiten desde el tercer país a responsables o encargados del tratamiento en el mismo tercer país[40].

d) Condiciones específicas para el tratamiento ulterior con otros fines (Artículo 9)

41. En cuanto al tratamiento ulterior o la comunicación de los datos transferidos desde la UE con fines distintos a los de aplicación de la ley, por ejemplo, por razones de seguridad nacional, también deben estar previstos por la ley, ser necesarios y proporcionados. También debe tenerse en cuenta la existencia de un mecanismo para informar a las autoridades competentes de los Estados miembros pertinentes de dicho tratamiento de datos ulterior[41]. También en este caso, una vez han sido objeto de tratamiento ulterior o se han comunicado, los datos deben gozar del mismo nivel de protección que cuando fueron tratados inicialmente por la autoridad competente receptora.

[35] Considerando 26 de la Directiva sobre protección de datos en el ámbito penal.
[36] Incluye las «las actuaciones policiales en las que no hay constancia de si un incidente es o no constitutivo de infracción penal. También pueden incluir el ejercicio de la autoridad mediante medidas coercitivas, como es el caso de las actuaciones policiales en manifestaciones, grandes acontecimientos deportivos y disturbios. Entre dichas actividades también figura el mantenimiento del orden público, como labor encomendada a la policía o, en su caso, a otras fuerzas y cuerpos de seguridad con fines de protección y prevención frente a las amenazas para la seguridad pública y para los intereses públicos fundamentales jurídicamente protegidos que puedan ser constitutivas de infracciones penales» (Considerando 12 de la Directiva sobre protección de datos en el ámbito penal). Debe distinguirse de un propósito de seguridad nacional o de las actividades incluidas en el ámbito de aplicación del título V, capítulo 2, del Tratado de la Unión Europea (TUE) (considerando 14 de la Directiva).
[37] Véase la nota a pie de página 33.
[38] Considerando 29 de la Directiva sobre protección de datos en el ámbito penal.
[39] Este mecanismo podría consistir, por ejemplo, en códigos de tratamiento mutuamente acordados, una obligación de notificación en virtud de un instrumento internacional, incluidas posibles notificaciones automatizadas, u otras medidas de transparencia similares.
[40] Considerando 64 de la Directiva sobre protección de datos en el ámbito penal.
[41] Véase la nota a pie de página 39.

e) El principio de minimización de los datos

42. Los datos deberán ser adecuados, pertinentes y no excesivos con respecto a los fines para los que se traten. En particular, debe tenerse en cuenta la aplicación de los requisitos de protección de los datos desde el diseño y por defecto, como los campos de entrada limitados (comunicaciones estructuradas) o los controles de calidad automatizados y no automatizados.

f) El principio de exactitud de los datos

43. Los datos deberán ser precisos y, en caso necesario, se mantendrán actualizados. No obstante, el principio de exactitud de los datos debe aplicarse teniendo presente el carácter y finalidad del tratamiento correspondiente. En particular en los procedimientos judiciales, las declaraciones que contienen datos personales se basan en la percepción subjetiva de las personas físicas y no siempre son verificables. En consecuencia, el requisito de exactitud no debe relacionarse con la exactitud de una afirmación, sino exclusivamente con el hecho de que se ha formulado una afirmación concreta[42].

44. Debe garantizarse que los datos personales que sean inexactos, incompletos o que no estén actualizados no se transmitan ni estén disponibles[43] y que se prevean procedimientos para corregir o eliminar los datos inexactos. En particular, deben tenerse en cuenta los sistemas de clasificación de la información tratada, en cuanto a la fiabilidad de la fuente y al nivel de verificación de los hechos[44].

g) El principio de retención de los datos

45. Los datos deben almacenarse durante un período no superior al necesario para los fines para los que se tratan. Deben establecerse mecanismos adecuados para la supresión de los datos personales; puede ser un periodo fijo o una revisión periódica de la necesidad de conservación de los datos personales (o una combinación de ambos): un período máximo fijo y una revisión periódica a determinados intervalos)[45]. Los datos personales almacenados durante periodos más largos para su archivo en interés público o para su uso científico, estadístico o histórico deben estar sujetos a las salvaguardias adecuadas (por ejemplo, en lo que respecta al acceso)[46].

h) El principio de seguridad y confidencialidad (Artículo 29, considerandos 28 y 71)

46. Toda entidad que trate datos personales debe asegurarse de que los datos personales son tratados de modo que se garantice un nivel adecuado de seguridad y confidencialidad, en particular impidiendo el acceso sin autorización a dichos datos o el uso no autorizado de los mismos y del equipo utilizado en el tratamiento. Esto incluye 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. A la hora de determinar el nivel de seguridad, deben tenerse en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como el riesgo de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

[42] Considerando 30 de la Directiva sobre protección de datos en el ámbito penal.
[43] Considerando 32 de la Directiva sobre protección de datos en el ámbito penal.
[44] Por ejemplo, rejillas 4x4 para evaluaciones de fiabilidad y códigos de tratamiento.
[45] Artículo 5 de la Directiva.
[46] Considerando 26 de la Directiva sobre protección de datos en el ámbito penal.

47. Deben garantizarse canales seguros de comunicación entre las autoridades de los Estados miembros que transfieren los datos personales y las autoridades receptoras de terceros Estados.

i) El principio de transparencia (Artículo 13, considerandos 26, 39, 42, 43, 44, 46)

48. Debe informarse a las personas físicas de los riesgos, reglas, salvaguardias y derechos aplicables en relación con el tratamiento de sus datos personales, así como del modo de hacer valer sus derechos en relación con dicho tratamiento[47].

49. Debe ponerse a disposición de las personas la información sobre todos los elementos principales del tratamiento de sus datos personales. Esta información debe ser fácilmente accesible y fácil de entender, para lo que debe emplearse un lenguaje claro y sencillo. Dicha información debe incluir los fines del tratamiento, la identidad del responsable, los derechos a su disposición[48] y otra información en la medida en que esto sea necesario para garantizar la lealtad.

50. Pueden existir algunas excepciones a este derecho de información. No obstante, dicha limitación debe estar permitida por una medida legislativa y ser necesaria y proporcionada para evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales, para no perjudicar la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, proteger la seguridad pública o la seguridad nacional o salvaguardar los derechos y las libertades de terceros, siempre y cuando dicha restricción parcial o completa constituya una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada. Estas restricciones también deben considerarse y evaluarse teniendo en cuenta la posibilidad de presentar una reclamación ante la autoridad de control y de interponer un recurso judicial. En cualquier caso, cualquier posible restricción debe ser temporal y no general, y debe estar limitada por condiciones, salvaguardias y limitaciones similares a las exigidas por la Carta y el CEDH, según los ha interpretado la jurisprudencia del Tribunal de Justicia y del Tribunal Europeo de Derechos Humanos, respectivamente, y, en particular, respetar la esencia de esos derechos y libertades.

j) Derecho de acceso, rectificación y supresión (Artículos 14 y 16)

51. El interesado debe tener derecho a obtener confirmación de si se están tratando o no datos personales que le conciernen y, en ese caso, tener acceso a sus datos. Este derecho debe incluir al menos cierta información sobre el tratamiento, como los fines y la base jurídica del tratamiento, el derecho a presentar una reclamación ante la autoridad de control o las categorías de datos personales de que se trate[49]. Esto es especialmente importante en el caso de que la transparencia se consiga mediante una notificación general (por ejemplo, información en el sitio web de la autoridad).

52. El interesado debe tener derecho a obtener la rectificación de sus datos por razones específicas, por ejemplo, cuando se demuestre que son inexactos o incompletos. El interesado también debe tener derecho a la supresión de sus datos cuando, por ejemplo, su tratamiento ya no sea necesario o sea ilícito.

53. El ejercicio de estos derechos no debe ser excesivamente complicado para el interesado.

[47] Considerando 26 de la Directiva sobre protección de datos en el ámbito penal.
[48] Tanto los derechos sustantivos (derecho de acceso, de rectificación, etc.) como el derecho de reparación.
[49] Artículo 14 de la Directiva.

k) Restricciones de los derechos de los interesados

54. Podrían existir posibles restricciones a estos derechos para evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales, para no perjudicar la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, proteger la seguridad pública o la seguridad nacional o salvaguardar los derechos y las libertades de terceros, siempre y cuando dicha restricción parcial o completa constituya una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada. Estas restricciones también deben considerarse y evaluarse teniendo en cuenta la posibilidad de presentar una reclamación ante la autoridad de control y de interponer un recurso judicial.

l) Restricción de las transferencias ulteriores (Artículo 35, considerandos 64-65)

55. Las transferencias ulteriores de datos personales por parte del destinatario inicial a otro tercer país u organización internacional no deben socavar el nivel de protección, previsto en la Unión, de las personas físicas cuyos datos se transfieren. Por lo tanto, estas transferencias de datos solo deben permitirse cuando se garantice la continuidad del nivel de protección que ofrece el Derecho de la UE[50]. En particular, el destinatario ulterior (es decir, el destinatario de la transferencia ulterior) debe ser una autoridad competente a efectos de aplicación de la ley[51] y dichas transferencias ulteriores de datos solo pueden tener lugar para fines limitados y específicos y siempre que exista un fundamento jurídico para ese tratamiento.

56. También debe tenerse en cuenta la existencia de un mecanismo para que las autoridades competentes del Estado miembro en cuestión sean informadas y autoricen dicha transferencia de datos. El destinatario inicial de los datos transferidos desde la UE debe ser responsable y poder demostrar que la autoridad competente pertinente del Estado miembro ha autorizado la transferencia ulterior[52] y que se ofrecen las garantías adecuadas para las transferencias ulteriores de datos en ausencia de una decisión de adecuación relativa al tercer país al que se transferirían los datos[53].

m) Principio de responsabilidad proactiva (Artículo 4, apartado 4)

57. El responsable del tratamiento será responsable y capaz de demostrar el cumplimiento de los principios de protección de datos que figuran en el artículo 4 de la Directiva.

[50] Véase también el Dictamen 1/15.
[51] Véase la nota a pie de página 33.
[52] En este contexto, debe tenerse en cuenta la existencia de una obligación o un compromiso de aplicar los códigos de tratamiento pertinentes definidos por las autoridades de los Estados miembros que realizan la transferencia.
[53] Los requisitos anteriores se entienden sin perjuicio de las condiciones específicas para las transferencias ulteriores a un país adecuado establecidas en la Directiva [artículo 35, apartado 1, letras c) y e)].

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

a) Categorías especiales de datos (Artículo 10 y considerando 37)

58. Deben existir garantías específicas cuando se trate de «categorías especiales de datos»[54], que aborden los riesgos específicos que conlleva[55]. Estas categorías deben reflejar las consagradas en el artículo 10 de la Directiva. Por lo tanto, el tratamiento de categorías especiales de datos debe estar sujeto a garantías específicas y solo se permitirá cuando sea estrictamente necesario en determinadas condiciones, por ejemplo, para proteger el interés vital de una persona.

b) Decisiones automatizadas y elaboración de perfiles (Artículo 11 y considerando 38)

59. Las decisiones basadas únicamente en el tratamiento automatizado (decisiones individuales automatizadas), incluida la elaboración de perfiles, que producen efectos legales adversos o que afectan considerablemente al interesado, solo se pueden adoptar en determinadas condiciones establecidas en el marco jurídico del tercer país[56].

60. En el marco de la Unión Europea, estas condiciones incluyen, por ejemplo, informar de forma específica al interesado, así como el derecho a la intervención humana por parte del responsable del tratamiento, en particular para que el interesado pueda expresar su punto de vista, obtener una explicación de la decisión adoptada tras dicha evaluación, o ejercer su derecho a impugnar la decisión.

61. En cualquier caso, el Derecho del tercer país debe establecer las garantías necesarias para los derechos y libertades del interesado. A este respecto, también debe tenerse en cuenta la existencia de un mecanismo para informar a las autoridades competentes del Estado miembro correspondiente de cualquier tratamiento ulterior, como el uso de los datos transferidos para la elaboración de perfiles a gran escala.

c) Protección de datos desde el diseño y por defecto (Artículo 20)

62. A la hora de evaluar la adecuación, debe prestarse atención a la existencia de la obligación de que los responsables del tratamiento adopten políticas internas y apliquen medidas que respeten, en particular, los principios de la protección de datos desde el diseño y de la protección de datos por defecto, teniendo en cuenta el estado de la técnica y el coste de la aplicación, y la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas planteados por el tratamiento, tanto en el momento de determinar los medios para el tratamiento como en el momento del propio tratamiento, y que adopten las medidas técnicas y organizativas apropiadas, como por ejemplo la seudonimización, concebidas para aplicar los principios de protección de datos, como por ejemplo la minimización de datos, de forma efectiva y para integrar las garantías necesarias en el tratamiento.

[54] Estas categorías especiales también se llaman «datos sensibles» en el considerando 37 de la Directiva.
[55] Estas garantías adicionales podrían ser, por ejemplo, medidas de seguridad específicas, derechos de acceso limitados para el personal, restricciones en cuanto al tratamiento ulterior, las decisiones automatizadas, el intercambio o las transferencias ulteriores.
[56] Dictamen 1/15, apartado 173.

C. Mecanismos relativos al procedimiento y la ejecución

63. 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 Europea[57], un sistema coherente con el europeo debe caracterizarse por la existencia de los siguientes elementos:

a) Autoridad de control independiente competente [Artículo 36, apartado 2, letra b), y apartado 3, y considerando 67]

64. 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 ejecutivos adecuados para garantizar el cumplimiento de los derechos de protección de datos y promover 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. También debe encargarse de asistir y asesorar a los interesados en el ejercicio de sus derechos [véase también el punto c) *infra*]. Las decisiones de adecuación deben determinar, en su caso, la autoridad o autoridades de control y los mecanismos de cooperación con las autoridades de control de los Estados miembros para hacer cumplir las normas de protección de datos.

b) Aplicación efectiva de las normas de protección de datos

65. El sistema del tercer país debe garantizar un elevado grado de 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 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.

66. 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. Dichas medidas deben incluir la llevanza de registros o archivos de registro de las actividades de tratamiento de datos durante un período de tiempo adecuado. También pueden incluir, por ejemplo, evaluaciones de impacto de la protección de datos, la designación de un delegado de protección de datos o la protección de datos desde el diseño y por defecto.

c) El sistema de protección de datos facilitará el ejercicio de los derechos del interesado (Artículos 12, 17 y 46 de la Directiva)

67. El marco de protección de datos de un tercer país debe obligar a los responsables del tratamiento a facilitar el ejercicio de los derechos de los interesados a los que se refiere la letra j) de la sección A, y disponer que su autoridad de control, previa solicitud, informe a los interesados sobre el ejercicio de sus derechos[58].

[57] Schrems I, apartado 74.
[58] El ejercicio de los derechos de los interesados puede ser directo o indirecto.

d) El sistema de protección de datos proporcionará mecanismos de reparación adecuados

68. Aunque actualmente no existe jurisprudencia en relación con la adecuación del sistema jurídico de un tercer país en virtud de la Directiva sobre protección de datos en el ámbito penal, el TJUE ha interpretado el derecho fundamental a la tutela judicial efectiva consagrado en el artículo 47 de la Carta. El primer apartado del artículo 47 de la Carta establece que toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva[59] respetando las condiciones establecidas en dicho artículo.

69. Según reiterada jurisprudencia, la existencia misma de un control jurisdiccional efectivo para garantizar el cumplimiento de las disposiciones del Derecho de la Unión es inherente a la existencia de un Estado de Derecho. Así, una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta[60].

70. 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.

71. 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.

72. Cuando no se cumplan las normas, también se ofrecerán al interesado cuyos datos se transfieren al tercer país mecanismos efectivos de reclamación administrativa y judicial en el tercer país, 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.

[59] El TJUE considera que la tutela judicial efectiva no solo la puede garantizar un órgano jurisdiccional, sino también un organismo que ofrezca garantías sustancialmente equivalentes a las exigidas en el artículo 47 de la Carta (véase Schrems II, apartado 197). Esto podría ser pertinente en particular para las organizaciones internacionales.
[60] Schrems II, apartados 187 y 194, incluida la jurisprudencia citada.