III

(Actos adoptados en aplicación del Tratado UE)

ACTOS ADOPTADOS EN APLICACIÓN DEL TÍTULO VI DEL TRATADO UE

DECISIÓN MARCO 2008/977/JAI DEL CONSEJO

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

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de la Unión Europea y, en particular, sus artículos 30 y 31 y su artículo 34, apartado 2, letra b),

Vista la propuesta de la Comisión,

Visto el dictamen del Parlamento Europeo [1],

Considerando lo siguiente:

(1) La Unión Europea se ha fijado el objetivo de mantener y desarrollar un espacio de libertad, seguridad y justicia en la Unión en el que debe ofrecerse un alto grado de seguridad mediante la acción en común de los Estados miembros en los ámbitos de la cooperación policial y judicial en materia penal.

(2) La acción en común en el ámbito de la cooperación policial de conformidad con el artículo 30, apartado 1, letra b), del Tratado de la Unión Europea y la acción en común sobre cooperación judicial en materia penal de conformidad con el artículo 31, apartado 1, letra a), del Tratado de la Unión Europea implican la necesidad de tratar la información pertinente ateniéndose a disposiciones adecuadas sobre protección de datos personales.

(3) La legislación en el ámbito del título VI del Tratado de la Unión Europea debe mejorar la cooperación policial y judicial en materia penal en cuanto a su eficacia y a su legitimidad y respeto de los derechos fundamentales, en particular el derecho a la intimidad y a la protección de los datos personales. La existencia de normas comunes para el tratamiento y la protección de los datos personales tratados con el fin de prevenir y luchar contra la delincuencia contribuye a la consecución de ambos objetivos.

(4) El Programa de La Haya sobre la consolidación de la libertad, la seguridad y la justicia en la Unión Europea, adoptado por el Consejo Europeo el 4 de noviembre de 2004, subrayaba la necesidad de un planteamiento innovador del intercambio transfronterizo de información policial, cumpliendo estrictamente condiciones fundamentales en el ámbito de la protección de datos, e invitaba a la Comisión a presentar propuestas a este respecto para finales de 2005 a más tardar. Ello se plasmó en el plan de acción del Consejo y la Comisión por el que se aplica el Programa de La Haya sobre el refuerzo de la libertad, la seguridad y la justicia en la Unión Europea [2].

(5) El intercambio de datos personales en el marco de la cooperación policial y judicial en materia penal, especialmente con arreglo al principio de disponibilidad de la información establecido en el Programa de La Haya, debe basarse en normas claras que aumenten la confianza mutua entre las autoridades competentes y garanticen la protección de la correspondiente información excluyendo toda discriminación respecto de esta cooperación entre los Estados miembros y garantizando al mismo tiempo el pleno respeto de los derechos fundamentales de la persona. Los instrumentos existentes a escala europea no bastan; la 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 [3], no se aplica al tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las contempladas en el título VI del Tratado de la Unión Europea, ni, en ningún caso, a las operaciones de tratamiento de datos relacionadas con la seguridad pública, la defensa, la seguridad del Estado o las actuaciones del Estado en materia penal.

[1] DO C 125 E de 22.5.2008, p. 154.

[2] DO C 198 de 12.8.2005, p. 1.

[3] DO L 281 de 23.11.1995, p. 31.

(6) La presente Decisión Marco se aplica únicamente a los datos recogidos o tratados por las autoridades competentes para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales y la ejecución de sanciones penales. La Decisión Marco debe dejar que sean los Estados miembros los que determinen de modo más preciso en el ámbito nacional qué otros fines deben considerarse incompatibles con el fin con el que se recopilaron inicialmente los datos personales. En términos generales, el tratamiento posterior de datos con fines históricos, estadísticos o científicos no debe considerarse incompatible con el fin inicial del tratamiento.

(7) El ámbito de aplicación de la Decisión Marco se limita al tratamiento de los datos personales transmitidos o puestos a disposición entre Estados miembros. De esta limitación no deben extraerse conclusiones relativas a la competencia de la Unión para adoptar actos relativos a la recopilación y tratamiento de datos personales en el ámbito nacional ni a la conveniencia de que la Unión tenga dicha competencia en el futuro.

(8) A fin de facilitar el intercambio de datos en la Unión, los Estados miembros desean garantizar que el nivel de protección logrado en el tratamiento de datos a nivel nacional coincida con el que se dispone en la presente Decisión Marco. Por lo que respecta al tratamiento nacional de datos, la presente Decisión Marco no impide que los Estados miembros establezcan garantías para la protección de los datos personales mayores a las contempladas en la presente Decisión Marco.

(9) La presente Decisión Marco no debe aplicarse a los datos personales que un Estado miembro haya obtenido en el ámbito de aplicación de la presente Decisión Marco y que tengan su origen en ese mismo Estado miembro.

(10) La aproximación de las disposiciones legales de los Estados miembros no debe debilitar la protección de datos que garantizan, sino que, por el contrario, debe tener por objeto garantizar un alto nivel de protección dentro de la Unión.

(11) Es necesario especificar los objetivos de la protección de datos en el marco de las actuaciones policiales y judiciales y establecer normas sobre la legalidad del tratamiento de datos personales, con el fin de garantizar que toda información que pueda intercambiarse se ha tratado lícitamente y de conformidad con los principios fundamentales relacionados con la calidad de los datos. Al mismo tiempo, no deben verse comprometidas en modo alguno las actuaciones legítimas de las autoridades policiales, aduaneras, judiciales y demás autoridades competentes.

(12) El principio de exactitud de los datos debe aplicarse teniendo presente el carácter y finalidad del tratamiento correspondiente. Por ejemplo, en particular en los procedimientos judiciales los datos se basan en apreciaciones subjetivas de la persona y, en algunos casos, son de imposible verificación. En consecuencia, el requisito de exactitud no puede relacionarse con la exactitud de una afirmación, sino exclusivamente con el hecho de que se ha formulado una afirmación concreta.

(13) El archivo en un conjunto independiente de datos solo debe permitirse si los datos ya no son necesarios ni utilizados para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. Debe también permitirse el archivo en un conjunto independiente de datos si los datos archivados se conservan en una base de datos junto con otros datos de manera tal que no pueden ya utilizarse con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. La adecuación del período de archivo debe depender de la finalidad del archivo y de los intereses legítimos de los interesados. Puede preverse un período muy largo en el caso del archivo con fines históricos.

(14) Los datos pueden también suprimirse mediante la destrucción de su soporte.

(15) Por lo que respecta a los datos inexactos, incompletos o anticuados transmitidos a otros Estados miembros o puestos a su disposición y tratados a continuación por autoridades cuasi judiciales —entendiéndose por tales las autoridades competentes para adoptar resoluciones jurídicamente vinculantes—, su rectificación, supresión o bloqueo debe efectuarse con arreglo al Derecho nacional.

(16) La garantía de un nivel elevado de protección de los datos personales de las personas requiere disposiciones comunes para determinar la licitud y la calidad de los datos tratados por las autoridades competentes de otros Estados miembros.

(17) Conviene definir a escala europea las condiciones en que debe permitirse a las autoridades competentes de los Estados miembros la transmisión a autoridades y particulares de los Estados miembros y puesta a su disposición de datos personales recibidos de otros Estados miembros. En muchos casos, la transmisión de datos personales a particulares por parte de los jueces, la policía o las aduanas es necesaria para enjuiciar infracciones penales o evitar una amenaza inmediata y grave a la seguridad pública o evitar que se lesionen gravemente los derechos de las personas, por ejemplo emitiendo alertas a los bancos y entidades de crédito en relación con la falsificación de valores o comunicando, en el ámbito de las delincuencia relacionada con vehículos, datos personales a las compañías de seguros a fin de impedir el tráfico ilícito de vehículos de motor robados o de mejorar las condiciones de recuperación de dichos vehículos en el extranjero. Esto no equivale al traspaso de funciones policiales o judiciales a particulares.

(18) Las normas de la presente Decisión Marco relativas a la transmisión de datos personales a particulares por parte de los jueces, la policía o las aduanas no se aplican a la comunicación de datos a particulares (como los abogados defensores o las víctimas) en el contexto del enjuiciamiento penal.

(19) El tratamiento posterior de los datos personales enviados o puestos a disposición por la autoridad competente de otro Estado miembro y, en particular, la transmisión o puesta a disposición posteriores de tales datos deben estar sujetos a normas comunes a escala europea.

(20) Cuando el tratamiento posterior de datos personales sea posible previo consentimiento del Estado miembro del que se hayan obtenido, cada Estado miembro debe poder determinar las modalidades de dicho consentimiento, incluso, por ejemplo, mediante un consentimiento general para categorías de información o categorías de tratamiento posterior.

(21) Cuando el tratamiento posterior de datos personales sea posible para procedimientos administrativos, dichos procedimientos también incluyen las actividades de los órganos de reglamentación y control.

(22) Las actividades legítimas de las autoridades policiales, aduaneras, judiciales y otras autoridades competentes pueden requerir que los datos se envíen a autoridades de terceros Estados u organismos internacionales que se encarguen de la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales.

(23) Cuando los datos personales se transfieren de un Estado miembro a terceros Estados o a organismos internacionales, dichos datos deben, en principio, gozar de un nivel de protección adecuado.

(24) Cuando los datos personales se transfieren de un Estado miembro a terceros países o a organismos internacionales, tal transferencia, en principio, únicamente debe efectuarse una vez que el Estados miembro del que se hayan obtenido los datos haya dado su consentimiento a la transferencia. Cada Estado miembro debe poder determinar las modalidades de dicho consentimiento, incluso, por ejemplo, mediante un consentimiento general para categorías de información o terceros Estados concretos.

(25) En el interés de una cooperación policial eficiente, cuando la naturaleza de una amenaza a la seguridad pública de un Estado miembro o de un tercer Estado sea lo bastante inmediata como para imposibilitar la obtención a tiempo del consentimiento previo, la autoridad competente debe poder transferir los datos personales correspondientes al tercer Estado de que se trate sin dicho consentimiento previo. Lo mismo podría ser de aplicación cuando estén en juego otros intereses esenciales de igual importancia de un Estado miembro, por ejemplo cuando exista una amenaza inmediata y grave a las infraestructuras vitales de un Estado miembro o cuando el sistema financiero de un Estado miembro pueda quedar gravemente perturbado.

(26) Puede ser necesario informar a los interesados sobre el tratamiento de sus datos, en particular en caso de que se hayan producido intromisiones graves en sus derechos debido a medidas de recogida secreta de datos, a fin de que el interesado pueda gozar de una protección jurídica eficaz.

(27) Los Estados miembros deben garantizar que se informe el interesado de que los datos personales pueden ser, o están siendo, recopilados, tratados o transmitidos a otro Estado miembro con fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales. El Derecho nacional debe determinar las modalidades del derecho del interesado a ser informado, así como las correspondientes excepciones. Esto puede hacerse de forma general, por ejemplo, por ley o por medio de la publicación de una lista de las operaciones de tratamiento.

(28) Para garantizar la protección de los datos personales sin comprometer el resultado de las investigaciones penales, es necesario definir los derechos del interesado.

(29) Algunos Estados miembros han establecido el derecho de acceso del interesado en materia penal mediante un sistema en que la autoridad nacional de control, en lugar del interesado, tiene acceso a todos los datos personales relativos al interesado sin restricción alguna y puede también rectificar, suprimir o actualizar los datos inexactos. En dicho caso de acceso indirecto, el Derecho nacional de dichos Estados miembros puede establecer que la autoridad nacional de control informe únicamente al interesado de la realización de todas las comprobaciones necesarias. No obstante, esos Estados miembros también establecen la posibilidad de acceso directo para el interesado en casos particulares, como el acceso a los registros judiciales, para obtener copia de sus propios antecedentes penales o de documentos referentes a sus propias declaraciones a los servicios de policía.

(30) Conviene establecer normas comunes sobre confidencialidad y seguridad del tratamiento, sobre responsabilidades y sanciones si las autoridades competentes hacen uso ilegal de los datos y sobre recursos judiciales a disposición del interesado. No obstante, corresponderá a cada Estado miembro determinar la naturaleza de sus normas sobre daños y las sanciones aplicables a las infracciones de las disposiciones nacionales sobre protección de datos.

(31) La presente Decisión Marco permite que cuando se apliquen los principios expuestos en la misma se tenga en cuenta el principio de acceso público a los documentos oficiales.

(32) De ser necesario para la protección de los datos personales en relación con un tratamiento que por sus dimensiones o su tipo suponga un riesgo específico para los derechos y libertades fundamentales, como por ejemplo el tratamiento por medio de tecnologías, mecanismos o procedimientos nuevos, es oportuno garantizar la consulta a las autoridades nacionales de control competentes antes de establecer los ficheros para el tratamiento de dichos datos.

(33) La creación en los Estados miembros de autoridades de control que ejerzan sus funciones con plena independencia constituye un aspecto esencial de la protección de datos personales tratados en el marco de la cooperación policial y judicial entre los Estados miembros.

(34) Las autoridades de control ya creadas en los Estados miembros en virtud de la Directiva 95/46/CE también deben poder asumir competencias sobre el cumplimiento de las funciones encomendadas a las autoridades nacionales de control que se creen en virtud de la presente Decisión Marco.

(35) Dichas autoridades de control deben disponer de los medios necesarios para cumplir sus funciones, entre ellos competencias de investigación y de intervención, en particular en casos de reclamaciones presentadas por particulares, y competencia para actuar en procedimientos judiciales. Tales autoridades de control deben contribuir a garantizar la transparencia de los tratamientos de datos en los Estados miembros de su competencia territorial. Sin embargo, sus competencias no deben afectar a las normas específicas previstas para los procesos penales, ni a la independencia del poder judicial.

(36) El artículo 47 del Tratado de la Unión Europea establece que ninguna de sus disposiciones afectará a los Tratados constitutivos de la Comunidad Europea ni a los Tratados y actos subsiguientes que los hayan modificado o completado. Por consiguiente, la presente Decisión Marco no afecta a la protección de datos personales regulada por el Derecho comunitario, tal como se establece en particular en la Directiva 95/46/CE, en el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos [1], y en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) [2].

(37) La presente Decisión Marco no afecta a las normas aplicables al acceso ilegal a los datos, establecidas en la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información [3].

(38) La presente Decisión Marco no afecta a las obligaciones y compromisos vigentes que incumban a los Estados miembros o a la Unión en virtud de acuerdos bilaterales o multilaterales con terceros Estados. Todo acuerdo futuro debe ser conforme a las normas sobre intercambios con terceros Estados.

(39) Varios actos adoptados en virtud del título VI del Tratado de la Unión Europea contienen disposiciones específicas sobre la protección de los datos personales intercambiados o tratados de otro modo en virtud de dichos actos. En algunos casos, estas disposiciones constituyen un conjunto completo y coherente de normas que abarcan todos los aspectos correspondientes de la protección de los datos (principios de calidad de los datos, normas sobre seguridad de los datos, reglamentación de los derechos y protecciones de los interesados, organización del control y responsabilidad), que reglamentan estos asuntos con más detalle que la presente Decisión Marco. Esta no debe afectar al conjunto pertinente de disposiciones de protección de datos de dichos actos, en particular a los que rigen el funcionamiento de Europol, Eurojust, el Sistema de Información de Schengen (SIS) y el Sistema de Información Aduanero (SIA), ni a los que permiten a las autoridades de los Estados miembros acceder directamente a determinados sistemas de datos de otros Estados miembros. Lo mismo se aplica a las disposiciones de protección de datos que rigen la transferencia automatizada de perfiles de ADN, datos dactiloscópicos y datos de los registros nacionales de matriculación de vehículos en virtud de la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza [4].

(40) En otros casos, las disposiciones sobre protección de datos que figuran en los actos adoptados en virtud del título VI del Tratado de la Unión Europea tienen un ámbito de aplicación más limitado. A menudo fijan condiciones particulares para el Estado miembro que recibe información que contenga datos personales de otros Estados miembros en cuanto a los fines para los que puede usar dichos datos, pero para otro aspectos de la protección de los datos se remite al Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal o al Derecho nacional. En la medida en que las disposiciones de estos actos que imponen condiciones a los Estados miembros receptores en cuanto al uso o posterior transferencia de datos personales sean más estrictas que las incluidas en las disposiciones correspondientes de la presente Decisión Marco, esta no debe afectará a las primeras. No obstante, para los demás aspectos deben aplicarse las normas establecidas en la presente Decisión Marco.

(41) La presente Decisión Marco no afecta al Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ni a su Protocolo adicional de 8 de noviembre de 2001, ni a los convenios del Consejo de Europa relativos a la cooperación judicial en materia penal.

[1] DO L 8 de 12.1.2001, p. 1.
[2] DO L 201 de 31.7.2002, p. 37.
[3] DO L 69 de 16.3.2005, p. 67.
[4] DO L 210 de 6.8.2008, p. 1.

(42) Dado que el objetivo de la presente Decisión Marco, a saber, la determinación de normas comunes para la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, no pueden ser alcanzados de manera suficiente por los Estados miembros y, por consiguiente, debido a las dimensión y los efectos de la acción, pueden lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado constitutivo de la Comunidad Europea y mencionado en el artículo 2 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad enunciado en el artículo 5 del Tratado constitutivo de la Comunidad Europea, la presente Decisión Marco no excede de lo necesario para alcanzar dicho objetivo.

(43) El Reino Unido participa en la presente Decisión, de conformidad con el artículo 5 del Protocolo por el que se integra el acervo de Schengen en el Marco de la Unión Europea, anejo al Tratado de la Unión Europea y al Tratado constitutivo de la Comunidad Europea, y de conformidad con el artículo 8, apartado 2, de la Decisión 2000/365/CE del Consejo, de 29 de mayo de 2000, sobre la solicitud del Reino Unido de Gran Bretaña e Irlanda del Norte de participar en algunas de las disposiciones del acervo de Schengen ([1]).

(44) Irlanda participa en la presente Decisión, de conformidad con el artículo 5 del Protocolo por el que se integra el acervo de Schengen en el Marco de la Unión Europea, anejo al Tratado de la Unión Europea y al Tratado constitutivo de la Comunidad Europea, y de conformidad con el artículo 6, apartado 2, de la Decisión 2002/192/CE del Consejo, de 28 de febrero de 2002, sobre la solicitud de Irlanda de participar en algunas de las disposiciones del acervo de Schengen ([2]).

(45) Por lo que se refiere a Islandia y Noruega, la presente Decisión Marco desarrolla disposiciones del acervo de Schengen, en el sentido del Acuerdo celebrado por el Consejo de la Unión Europea con la República de Islandia y el Reino de Noruega sobre la asociación de estos dos Estados a la ejecución, aplicación y desarrollo del acervo de Schengen ([3]), que entran en el ámbito mencionado en el artículo 1, puntos H e I, de la Decisión 1999/437/CE del Consejo ([4]), relativa a determinadas normas de desarrollo de dicho Acuerdo.

(46) Por lo que se refiere a Suiza, la presente Decisión Marco desarrolla disposiciones del acervo de Schengen, en el sentido del Acuerdo celebrado entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de este Estado a la ejecución, aplicación y desarrollo del acervo de Schengen ([5]), que entran en el ámbito mencionado en el artículo 1, puntos H e I, de la Decisión 1999/437/CE, en relación con el artículo 3 de la Decisión 2008/149/JAI del Consejo ([6]), relativa a la celebración de dicho Acuerdo en nombre de la Unión Europea.

(47) Por lo que se refiere a Liechtenstein, la presente Decisión Marco desarrolla disposiciones del acervo de Schengen, en el sentido del Protocolo entre la Unión Europea, la Comunidad Europea, la Confederación Suiza y el Principado de Liechtenstein sobre la adhesión del Principado de Liechtenstein al Acuerdo entre la Unión Europea, la Comunidad Europea y la Confederación Suiza sobre la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen, que entran en el ámbito mencionado en el artículo 1, puntos H e I, de la Decisión 1999/437/CE, en relación con el artículo 3 de la Decisión 2008/262/JAI del Consejo ([7]), relativa a la celebración de dicho Acuerdo en nombre de la Unión Europea.

(48) La presente Decisión Marco respeta los derechos fundamentales y los principios reconocidos, en particular por la Carta de los Derechos Fundamentales de la Unión Europea ([8]). La presente Decisión Marco pretende garantizar el pleno respeto del derecho a la intimidad y a la protección de los datos de carácter personal reflejados en los artículos 7 y 8 de la Carta.

HA ADOPTADO LA PRESENTE DECISIÓN MARCO:

Artículo 1

Objetivo y ámbito de aplicación

1. El objetivo de la presente Decisión Marco es garantizar un alto nivel de protección de los derechos y libertades fundamentales de las personas físicas y en particular su derecho a la intimidad en lo que respecta al tratamiento de datos personales en el marco de la cooperación policial y judicial en materia penal, contemplada en el título VI del Tratado de la Unión Europea, garantizando al mismo tiempo un alto nivel de seguridad pública.

2. De conformidad con lo establecido en la presente Decisión Marco, los Estados miembros protegerán los derechos y libertades fundamentales de las personas físicas, y en particular su derecho a la intimidad, cuando, para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o para la ejecución de sanciones penales los datos personales:

a) los Estados miembros los transmitan o hayan transmitido o los pongan o hayan puesto a disposición entre sí;

([1]) DO L 131 de 1.6.2000, p. 43.
([2]) DO L 64 de 7.3.2002, p. 20.
([3]) DO L 176 de 10.7.1999, p. 36.
([4]) DO L 176 de 10.7.1999, p. 31.
([5]) DO L 53 de 27.2.2008, p. 52.
([6]) DO L 53 de 27.2.2008, p. 50.
([7]) DO L 83 de 26.3.2008, p. 5.
([8]) DO C 303 de 14.12.2007, p. 1.

b) los Estados miembros los transmitan o hayan transmitido a autoridades o sistemas de información creados en virtud del título VI del Tratado de la Unión Europea, o los pongan o hayan puesto a su disposición, o

c) las autoridades o sistemas de información creados en virtud del Tratado de la Unión Europea o del Tratado constitutivo de la Comunidad Europea los transmitan o hayan transmitido a las autoridades competentes de los Estados miembros, o los pongan o hayan puesto a su disposición.

3. La presente Decisión Marco se aplicará tanto al tratamiento automatizado como no automatizado, total o parcial, de datos personales que formen parte o esté previsto que vayan a formar parte de un fichero.

4. La presente Decisión Marco no afectará a los intereses esenciales de seguridad del Estado ni a las actividades específicas de inteligencia en el sector de la seguridad del Estado.

5. La presente Decisión Marco no impedirá a los Estados miembros establecer, para la protección de los datos personales recopilados o tratados a nivel nacional, garantía mayores a las establecidas en la presente Decisión Marco.

Artículo 2

Definiciones

A efectos de la presente Decisión Marco, se entenderá por:

a) «datos personales», toda información sobre una persona física identificada o identificable («el interesado»). Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;

b) «tratamiento de datos personales» y «tratamiento», cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;

c) «bloqueo», la señalización de datos personales conservados con el objetivo de limitar su tratamiento en el futuro;

d) «fichero de datos personales» y «fichero», todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

e) «encargado del tratamiento», todo organismo que trate datos personales por cuenta del responsable del tratamiento;

f) «destinatario», todo organismo al que se comuniquen datos;

g) «consentimiento del interesado», toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consiente el tratamiento de datos personales que le conciernan.

h) «autoridades competentes», los servicios u organismos creados en virtud de actos jurídicos adoptados por el Consejo al amparo del título VI del Tratado de la Unión Europea, así como las autoridades policiales, judiciales, aduaneras y otras autoridades competentes de los Estados miembros autorizadas por el Derecho nacional a tratar datos personales en el ámbito de la presente Decisión Marco;

i) «responsable del tratamiento», la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales;

j) «marcado», la señalización de datos personales conservados sin el objetivo de limitar su tratamiento en el futuro;

k) «procedimiento de disociación», la modificación de datos personales de manera que los detalles de las condiciones personales o materiales no puedan ya atribuirse a una persona física identificada o identificable, o solo sea posible invirtiendo tiempo, costes y trabajo desproporcionados.

Artículo 3

Principios de licitud, proporcionalidad y finalidad

1. Las autoridades competentes solo podrán recoger datos personales con fines determinados, explícitos y legítimos en el marco de sus funciones y solo podrán tratarlos para el mismo fin con el que se hayan recogido. El tratamiento de los datos deberá ser lícito y adecuado, pertinente y no excesivo con respecto a los fines para los que se recojan.

2. Se autorizará el tratamiento posterior para otros fines en la medida en que:

a) el tratamiento no sea incompatible con los fines para los que se recogieron los datos;

b) las autoridades competentes estén autorizadas a tratar los datos para tales otros fines con arreglo a la normativa aplicable, y

c) el tratamiento sea necesario para ese otro fin y proporcionado a él.

Las autoridades competentes podrán también tratar posteriormente los datos personales transmitidos con fines históricos, estadísticos o científicos, siempre que los Estados miembros dispongan las garantías adecuadas, como la disociación de los datos.

Artículo 4

Rectificación, supresión y bloqueo

1. Los datos personales se rectificarán cuando sean incorrectos y, cuando sea posible y necesario, se completarán o actualizarán.

2. Los datos personales se suprimirán o disociarán cuando ya no sean necesarios a los fines para los que fueron legalmente recogidos o legalmente tratados posteriormente. Esta disposición no afectará al archivo de dichos datos en conjunto independiente de datos durante un período adecuado de tiempo realizado de acuerdo con el Derecho nacional.

3. Los datos personales se bloquearán, en lugar de suprimirse, en caso de que haya razones justificadas para suponer que la supresión pueda perjudicar los intereses legítimos del interesado. Los datos bloqueados podrán tratarse solo para los fines que impidieron su supresión.

4. Si los datos personales forman parte de una resolución judicial o registro relacionado con el pronunciamiento de una resolución judicial, la rectificación, supresión o bloqueo se efectuará de conformidad con la normativa nacional sobre procedimientos judiciales.

Artículo 5

Fijación de plazos de supresión y comprobación

Se fijarán plazos adecuados a efectos de la supresión de datos personales o de la comprobación periódica de la necesidad de su conservación. Se garantizará el cumplimiento de los plazos mediante disposiciones de procedimiento.

Artículo 6

Tratamiento de categorías especiales de datos

El tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, de datos relativos a la salud o a la vida sexual solo se permitirá cuando sea estrictamente necesario y si el Derecho nacional establece garantías adecuadas.

Artículo 7

Decisiones específicas automatizadas

Las decisiones que produzcan efectos jurídicos adversos en el interesado o le afecten de manera significativa y que se basen únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad solo se permitirán cuando estén autorizadas por una ley que a su vez establezca medidas que garanticen los intereses legítimos del interesado.

Artículo 8

Control de calidad de los datos transmitidos o disponibles

1. Las autoridades competentes adoptarán todas las medidas razonables para disponer que los datos personales que sean inexactos, incompletos o que no estén actualizados no se transmitan ni se hagan disponibles. Para ello, las autoridades competentes, en la medida en que sea factible, controlarán la calidad de los datos personales antes de transmitirlos o hacerlos disponibles. En la medida de lo posible, en todas las transmisiones de datos se deberá añadir la información de que se disponga para que el Estado miembro receptor pueda valorar el grado en que los datos son exactos, completos, actualizados y fiables. Si se hubieran transmitido datos personales sin haberlos solicitado la autoridad receptora, esta comprobará sin demora si los datos son necesarios para el fin para el cual se transmitieron.

2. Si se observara que se hubieran transmitido datos incorrectos o se hubieran transmitido ilegalmente, el hecho se pondrá de inmediato en conocimiento del destinatario. Esos datos deberán rectificarse, suprimirse o bloquearse de inmediato de conformidad con el artículo 4.

Artículo 9

Plazos

1. Al transmitir o poner a disposición los datos, la autoridad transmisora podrá indicar, ateniéndose a su Derecho nacional y de conformidad con los artículos 4 y 5, los plazos fijados para la retención de los datos, a cuya expiración el destinatario deberá suprimirlos o bloquearlos o comprobar si siguen siendo necesarios. Esta obligación no se aplicará si, en el momento en que expiren dichos plazos, los datos son necesarios para una investigación en curso, el enjuiciamiento de infracciones penales o la ejecución de sanciones penales.

2. Si la autoridad transmisora no hubiera indicado ningún plazo de conformidad con el apartado 1, se aplicarán los plazos mencionados en los artículos 4 y 5 para la retención de los datos establecidos en el Derecho nacional del Estado miembro receptor.

Artículo 10

Registro y documentación

1. Toda transmisión de datos personales se registrará o documentará a efectos de comprobación de la licitud de su tratamiento, de autocontrol y de garantía de su integridad y seguridad.

2. Los registros o documentación realizados de conformidad con el apartado 1 se comunicarán a petición de la autoridad de control competente para el control de la protección de datos. La autoridad de control competente utilizará esa información únicamente para el control de la protección de datos y para garantizar el adecuado tratamiento de los datos y la integridad y seguridad de estos.

Artículo 11

Tratamiento de datos personales transmitidos o puestos a disposición por otro Estado miembro

Los datos personales transmitidos o puestos a disposición por la autoridad competente de otro Estado miembro únicamente podrán tratarse posteriormente, de conformidad con los requisitos del artículo 3, apartado 2, para los siguientes fines distintos de aquellos para los que se transmitieron o pusieron a disposición:

a) la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales distintas de aquellas para las que se transmitieron o pusieron a disposición;

b) otros procedimientos judiciales y administrativos directamente relacionados con la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales;

c) la prevención de amenazas inmediatas y graves a la seguridad pública, o

d) cualquier otro fin, solo con el previo consentimiento del Estado miembro transmisor o con el consentimiento del interesado, otorgados de acuerdo con el Derecho nacional.

Las autoridades competentes también podrán tratar posteriormente con fines históricos, estadísticos o científicos los datos personales transmitidos, a condición de que los Estados miembros establezcan las garantías adecuadas, como, por ejemplo, la disociación de los datos.

Artículo 12

Cumplimiento de las limitaciones nacionales de tratamiento

1. Cuando, con arreglo al Derecho del Estado miembro transmisor, se apliquen limitaciones específicas de tratamiento en circunstancias concretas a los intercambios de datos entre autoridades competentes en dicho Estado miembro, la autoridad transmisora comunicará al destinatario dichas limitaciones. El destinatario garantizará que se cumplan dichas limitaciones de tratamiento.

2. Al aplicar el apartado 1, los Estados miembros no aplicarán, en relación con las transmisiones de datos a otros Estados miembros o a los servicios u organismos creados en virtud del título VI del Tratado de la Unión Europea, más restricciones que las aplicables a las transmisiones similares de datos a escala nacional.

Artículo 13

Transferencia a autoridades competentes de terceros Estados y a organismos internacionales

1. Los Estados miembros dispondrán que los datos personales transmitidos o puestos a disposición por la autoridad competente de otro Estado miembro puedan transferirse a terceros Estados u organismos internacionales solo si se cumplen todas las condiciones siguientes:

a) que sea necesario para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o para la ejecución de sanciones penales;

b) que la autoridad receptora del tercer Estado o el organismo internacional receptor sea competente para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales;

c) que el Estado miembro que proporcionó los datos haya consentido la transferencia de acuerdo con su Derecho nacional;

d) que el tercer Estado u organismo internacional de que se trate garantice un nivel adecuado de protección en el tratamiento de datos previsto.

2. La transferencia de datos sin el consentimiento previo de acuerdo con el apartado 1, letra c), solo podrá permitirse si es esencial para la prevención de una amenaza inmediata y grave a la seguridad pública de un Estado miembro o de un tercer Estado o a intereses esenciales de un Estado miembro, y si el consentimiento previo no puede obtenerse a tiempo. Se informará sin demora a la autoridad encargada de otorgar el consentimiento.

3. No obstante lo dispuesto en el apartado 1, letra d), podrán transferirse datos personales en cualquiera de los siguientes supuestos:

a) que así lo disponga el Derecho nacional del Estado miembro que transfiere los datos por alguno de los siguientes motivos:

   i) legítimos intereses específicos del interesado, o

   ii) legítimos intereses superiores, en especial importantes intereses públicos, o

b) que el tercer Estado o el organismo internacional receptor ofrezca garantías que el Estado miembro de que se trate considere adecuadas de conformidad con su Derecho nacional.

4. La adecuación del nivel de protección a que se refiere el apartado 1, letra d), se evaluará atendiendo a todas las circunstancias que concurran en una operación de transferencia de datos o en un conjunto de operaciones de transferencia de datos. Se tomará en consideración en particular la naturaleza de los datos, la finalidad y la duración de la operación u operaciones de tratamiento previstas, el Estado de origen y el Estado u organismo internacional de destino final de los datos, la normativa, tanto general como sectorial, vigente en el tercer Estado u organismo internacional de que se trate, y las normas profesionales y medidas de seguridad que sean de aplicación.

Artículo 14

Transmisión a particulares en los Estados miembros

1. Los Estados miembros dispondrán que los datos personales recibidos de las autoridades competentes de otro Estado miembro o que aquellas hayan puesto su disposición solo puedan transmitirse a particulares si se cumplen las condiciones siguientes:

a) que la autoridad competente del Estado miembro del que se obtuvieron los datos haya consentido en que estos se transmitan de acuerdo con su Derecho nacional;

b) que los legítimos intereses específicos del interesado no impidan la transmisión;

c) que en determinados casos sea esencial que la autoridad competente transmita los datos a particulares por alguno de los siguientes motivos:

i) para el cumplimiento de funciones que tiene legalmente asignadas,

ii) para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales,

iii) para la prevención de amenazas inmediatas y graves a la seguridad pública, o

iv) para la prevención de lesiones graves de los derechos de las personas.

2. La autoridad competente que transmita datos a un particular informará a este de los fines para los que podrán utilizarse exclusivamente los datos.

Artículo 15

Información a petición de las autoridades competentes

Si así se lo solicitan, el destinatario informará sobre el tratamiento de los datos a las autoridades competentes que le hayan transmitido o puesto a su disposición los datos personales.

Artículo 16

Información al interesado

1. Los Estados miembros se harán cargo de que el interesado esté informado de lo relativo a la recopilación o tratamiento de datos personales por sus autoridades competentes, conforme al Derecho nacional.

2. En caso de haberse transmitido o puesto a disposición entre Estado miembro datos personales, cada Estado miembro podrá, de conformidad con las disposiciones de su Derecho nacional a que se refiere el apartado 1, pedir que el otro Estado miembro se abstenga de informar al interesado. En tal caso, este último Estado miembro no informará al interesado sin el consentimiento previo del primero.

Artículo 17

Derecho de acceso a los datos

1. Todo interesado que lo solicite con una periodicidad razonable tendrá derecho a obtener, sin restricciones y sin retrasos ni gastos excesivos:

a) al menos la confirmación, por parte del responsable del tratamiento o de la autoridad nacional de control, de que se han transmitido o puesto a disposición datos que le conciernen, e información sobre los destinatarios o categorías de destinatarios a los que se han remitido los datos y la comunicación de los datos que se están tratando, o

b) al menos la confirmación de la autoridad nacional de control de que se han realizado todas las comprobaciones necesarias.

2. Los Estados miembros podrán adoptar medidas legislativas para limitar el acceso a la información de acuerdo con el apartado 1, letra a), cuando tal limitación, habida debida cuenta de los intereses legítimos del interesado, constituya una medida necesaria y proporcionada:

a) para evitar que se obstaculicen investigaciones o procedimientos jurídicos o de carácter oficial;

b) para evitar que se obstaculice la prevención, detección, investigación y enjuiciamiento de infracciones penales o la ejecución de sanciones penales;

c) para proteger la seguridad pública;

d) para proteger la seguridad del Estado;

e) para proteger al interesado o los derechos y libertades de terceros.

3. Toda denegación o limitación del acceso se comunicará al interesado por escrito. Se comunicarán al mismo tiempo los motivos materiales o jurídicos en que se basa la decisión. Esta última comunicación podrá omitirse cuando exista algún motivo de los indicados en el apartado 2, letras a) a e). En todos estos casos se pondrá en conocimiento del interesado que puede recurrir ante la autoridad nacional de control o los juzgados o tribunales competentes.

Artículo 18

Derecho de rectificación, supresión o bloqueo

1. El interesado tendrá derecho al cumplimiento, por parte del responsable del tratamiento, de sus obligaciones —de conformidad con los artículos 4, 8 y 9— de rectificación, supresión y bloqueo de datos personales, derivadas de la presente Decisión Marco. Los Estados miembros establecerán si el interesado puede invocar este derecho directamente ante el responsable del tratamiento de los datos o por mediación de la autoridad nacional de control competente. Si el responsable del tratamiento deniega la rectificación, supresión o bloqueo, la denegación deberá comunicarse por escrito al interesado, al que se deberá informar de las posibilidades de reclamación o de recurso jurisdiccional establecidas en el Derecho nacional. Al examinarse la reclamación o el recurso jurisdiccional se informará al interesado de si fue correcta o incorrecta la actuación del responsable del tratamiento. Los Estados miembros podrán también disponer que la autoridad nacional de control competente informe al interesado que se ha procedido a una revisión.

2. Si el interesado contesta la exactitud de un dato personal y no se puede determinar si este es exacto o inexacto, podrá marcarse dicho dato.

Artículo 19

Derecho a reparación

1. Toda persona que haya sufrido daños y perjuicios como consecuencia del tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Decisión Marco, tendrá derecho a obtener reparación por los mismos del responsable del tratamiento o de otra autoridad competente de acuerdo con el Derecho nacional.

2. Si una autoridad competente de un Estado miembro transmitió datos personales, el destinatario no podrá, en el ámbito de sus responsabilidades ante la parte perjudicada de conformidad con el Derecho nacional, alegar en su defensa que los datos transmitidos eran inexactos. Si el destinatario repara los daños y perjuicios causados por el uso de datos inexactos transmitidos, la autoridad competente transmisora abonará al destinatario el importe pagado en concepto de daños y perjuicios, teniendo en cuenta cualquier responsabilidad que pueda imputarse al destinatario.

Artículo 20

Vías de recurso

Sin perjuicio del recurso administrativo que pueda interponerse antes de acudir a la autoridad judicial, el interesado tendrá derecho a un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables.

Artículo 21

Confidencialidad del tratamiento

1. Las personas que tengan acceso a datos personales que entren en el ámbito de aplicación de la presente Decisión Marco solo podrán tratarlos si pertenecen a la autoridad competente o siguiendo instrucciones de esta, o salvo en virtud de un imperativo legal.

2. Las personas que trabajen para una autoridad competente de un Estado miembro estarán sometidos a todas las normas de protección de datos que rijan para esa autoridad competente.

Artículo 22

Seguridad del tratamiento

1. Los Estados miembros establecerán la obligación de las autoridades competentes de aplicar las medidas técnicas y de organización adecuadas para proteger los datos personales contra la destrucción accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red o la puesta a disposición de datos mediante acceso automatizado directo, y contra cualquier otro tratamiento ilícito, teniendo en cuenta en particular los riesgos que presente el tratamiento y la naturaleza de los datos que deban protegerse. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

2. Por lo que se refiere al tratamiento automatizado de datos, cada Estado miembro aplicará medidas destinadas a:

a) impedir el acceso de personas no autorizadas a las instalaciones utilizadas para el tratamiento de datos personales (control de acceso a las instalaciones);

b) impedir que los soportes de datos puedan ser leídos, copiados, modificados o retirados sin autorización (control de los soportes de datos);

c) impedir que se introduzcan datos sin autorización en los ficheros y que puedan conocerse, modificarse o suprimirse sin autorización datos personales conservados (control de la conservación);

d) impedir que los sistemas de tratamiento automatizado de datos puedan ser utilizados por personas no autorizadas mediante equipos de transmisión de datos (control de la utilización);

e) garantizar que las personas autorizadas para utilizar un sistema de tratamiento automatizado de datos solo puedan tener acceso a los datos para los que se les ha autorizado (control del acceso);

f) garantizar que sea posible verificar y comprobar a qué organismos se han transmitido o pueden transmitirse o a cuya disposición pueden ponerse datos personales mediante equipos de transmisión de datos (control de las comunicaciones);

g) garantizar que pueda verificarse y comprobarse *a posteriori* qué datos personales se han introducido en los sistemas de tratamiento automatizado de datos y en qué momento y por qué persona han sido introducidos (control de la introducción);

h) impedir que durante la transmisión de datos personales y durante el transporte de soportes de datos, los datos puedan ser leídos, copiados, modificados o suprimidos sin autorización (control del transporte);

i) garantizar que los sistemas utilizados puedan repararse en caso de fallo del sistema (recuperación);

j) garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados (fiabilidad) y que los datos conservados no se degraden por fallos de funcionamiento del sistema (integridad).

3. Los Estados miembros establecerán que solo pueda designarse como encargado del tratamiento quien garantice el cumplimiento de las medidas técnicas y de organización contempladas en el apartado 1 y de las instrucciones en virtud del artículo 21. La autoridad competente controlará al respecto al encargado del tratamiento.

4. El encargado del tratamiento solo podrá tratar los datos personales en virtud de acto jurídico o de contrato escrito.

Artículo 23

Consulta previa

Los Estados miembros garantizarán que se consulte a las autoridades nacionales de control competentes antes del tratamiento de datos personales que vayan a formar parte de un nuevo sistema que vaya a crearse, en cualquiera de los siguientes casos:

a) que vayan a tratarse las categorías especiales de datos contempladas en el artículo 6, o

b) que el tipo de tratamiento, en particular mediante tecnologías, mecanismos o procedimientos nuevos, entrañe otro tipo de riesgos específicos para los derechos y libertades fundamentales y, en particular, para la intimidad del interesado.

Artículo 24

Sanciones

Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de lo dispuesto en la presente Decisión Marco y establecerán, en particular, sanciones eficaces, proporcionadas y disuasorias, que se impondrán en caso de incumplimiento de las disposiciones adoptadas en virtud de la presente Decisión Marco.

Artículo 25

Autoridades nacionales de control

1. Cada Estado miembro dispondrá que una o más autoridades públicas se encarguen en su territorio de asesorar y vigilar la aplicación de las disposiciones que los Estados miembros hayan adoptado en aplicación de la presente Decisión Marco. Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.

2. La autoridad de control dispondrá, en particular, de:

a) poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control;

b) poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos y garantizar una publicación adecuada de dichos dictámenes, el de ordenar el bloqueo, la supresión o la destrucción de datos, el de prohibir provisional o definitivamente un tratamiento, el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales;

c) capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Decisión Marco o de poner dichas infracciones en conocimiento de la autoridad judicial. Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional.

3. Toda autoridad de control entenderá de las solicitudes que cualquier persona le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud.

4. Los Estados miembros dispondrán que los miembros y agentes de las autoridades de control deberán observar las normas de protección de datos aplicables a la autoridad competente correspondiente y que, incluso después de haber cesado en sus funciones, estarán sujetos al deber de secreto profesional sobre informaciones confidenciales a la que hayan tenido acceso.

Artículo 26

Relación con acuerdos con terceros Estados

La presente Decisión Marco no afectará a las obligaciones y compromisos contraídos por los Estados miembros o la Unión en virtud de acuerdos bilaterales o multilaterales con terceros Estados que estén vigentes en el momento de la adopción de la presente Decisión Marco.

Al aplicar los citados acuerdos, la transferencia a un tercer Estado de datos personales obtenidos de otro Estado miembro se llevará a cabo de conformidad con lo dispuesto en el artículo 13, apartado 1, letra c), o apartado 2, según proceda.

Artículo 27

Evaluación

1. A más tardar el 27 de noviembre de 2013, los Estados miembros informarán a la Comisión sobre las medidas nacionales que hayan adoptado para dar pleno cumplimiento a la presente Decisión Marco, y en particular sobre aquellas disposiciones que deben cumplirse ya cuando se procede a la recogida de los datos. La Comisión estudiará, en particular, las repercusiones de dichas disposiciones en el ámbito de aplicación de la presente Decisión Marco establecido en el artículo 1, apartado 2.

2. La Comisión informará en el plazo de un año al Parlamento Europeo y al Consejo sobre los resultados de la evaluación a que se refiere el apartado 1 y acompañará el informe con las propuestas de modificación de la presente Decisión Marco que sean adecuadas.

Artículo 28

Relación con actos de la Unión adoptados previamente

Cuando algún acto, adoptado en virtud del título VI del Tratado de la Unión Europea antes de la fecha de entrada en vigor de la presente Decisión Marco y que regule el intercambio de datos personales entre los Estados miembros o el acceso de unas autoridades designadas de los Estados miembros a sistemas de información establecidos en virtud del Tratado constitutivo de la Comunidad Europea, establezca condiciones específicas respecto de la utilización de dichos datos por el Estado miembro receptor, estas primarán sobre las disposiciones de la presente Decisión Marco relativas al uso de los datos transmitidos o puestos a disposición por otro Estado miembro.

Artículo 29

Aplicación

1. Los Estados miembros adoptarán las medidas necesarias para dar cumplimiento a lo dispuesto en la presente Decisión Marco antes del 27 de noviembre de 2010.

2. A más tardar en la misma fecha, los Estados miembros transmitirán a la Secretaría General del Consejo y a la Comisión el texto de las disposiciones de adaptación de su Derecho nacional en virtud de las obligaciones derivadas de la presente Decisión Marco, así como información sobre la designación de las autoridades de control a que se refiere el artículo 25. Basándose en un informe redactado por la Comisión utilizando dicha información, el Consejo evaluará, antes del 27 de noviembre de 2011, la medida en que los Estados miembros han cumplido lo dispuesto en la presente Decisión Marco.

Artículo 30

Entrada en vigor

La presente Decisión Marco entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en Bruselas, el 27 de noviembre de 2008.

Por el Consejo

La Presidenta

M. ALLIOT-MARIE