COMISIÓN DE LAS COMUNIDADES EUROPEAS

Bruselas, 4.10.2005
COM(2005) 475 final

2005/0202 (CNS)

Propuesta de

DECISIÓN MARCO DEL CONSEJO

relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal

{SEC(2005) 1241}

(presentada por la Comisión)

EXPOSICIÓN DE MOTIVOS

1) CONTEXTO DE LA PROPUESTA

- **Motivación y objetivos de la propuesta**

El 4 de noviembre de 2004, el Consejo Europeo adoptó el Programa de La Haya sobre la consolidación de la libertad, la seguridad y la justicia en la Unión Europea.[1] En este Programa se invita a la Comisión a que presente propuestas antes de finales de 2005 para la aplicación del principio de disponibilidad, con el fin de mejorar el intercambio transfronterizo de información policial entre los Estados miembros. El Programa de La Haya destaca que en estas propuestas deben cumplirse una serie de condiciones imprescindibles en el ámbito de la protección de datos.

En junio de 2005, el Consejo y la Comisión adoptaron el Plan de Acción por el que se aplica el Programa de la Haya.[2] Se basaba en la Comunicación de la Comisión al Consejo y al Parlamento Europeo - Programa de la Haya: Diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia.[3] De conformidad con el Plan de Acción, la Comisión presentará propuestas en *2005 sobre 1) la instauración de un principio de disponibilidad de la información pertinente en el marco de la represión de actividades ilícitas y 2) sobre garantías adecuadas para la transferencia de datos personales a efectos de cooperación policial y judicial en asuntos penales.* El 13 de julio de 2005, el Consejo (Justicia y Asuntos de Interior), en su Declaración sobre la respuesta de la UE a los atentados de Londres[4], invitó a la Comisión a presentar estas propuestas para octubre de 2005.

La presente Decisión marco garantizará la protección de los datos personales tratados en el marco de la cooperación policial y judicial en materia penal entre los Estados miembros de la Unión Europea (TUE, título VI). Su objetivo es mejorar esta cooperación, en particular por lo que respecta a la prevención y la lucha contra el terrorismo, cumpliendo estrictamente condiciones imprescindibles en el ámbito de la protección de datos. Garantizará el respeto de los derechos fundamentales en la Unión Europea, especialmente el derecho a la intimidad y a la protección de datos personales, con vistas a la aplicación del principio de disponibilidad, y evitará que el intercambio de información pertinente entre los Estados miembros se vea obstaculizado por la existencia en ellos de niveles diferentes de protección de datos.

- **Contexto general**

A raíz de una iniciativa de Italia[5], la protección de datos personales en el tercer pilar ya se había debatido en 1998. En aquel momento, el Consejo de Justicia y Asuntos de Interior adoptó el denominado Plan de acción de Viena[6]. Establecía que, por lo que se refiere a las cuestiones horizontales en el contexto de la cooperación policial y judicial en materia penal, deberían estudiarse las posibilidades de normas armonizadas sobre protección de datos en un plazo de dos años a partir de la entrada en vigor del Tratado. Sin embargo, en 2001 no pudo adoptarse un proyecto de Resolución relativa a las normas sobre protección de datos

---

1 DO C 53 de 3.3.2005, p. 1.
2 DO C 198 de 12.8.2005, p. 1.
3 COM(2005) 184 final, Bruselas, 10.5.2005.
4 Documento de trabajo del Consejo 11158/1/05 REV 1 JAI 255.
5 Documento de trabajo del Consejo 8321/98JAI 15.
6 DO C 19 de 23.1.1999, p. 1.

personales en los instrumentos del tercer pilar de la Unión Europea[7]. En junio de 2003, la Presidencia griega propuso un conjunto de principios generales en relación con la protección de datos personales en el marco del tercer pilar[8] que se inspiraban en la Directiva 95/46/CE sobre protección de datos y en la Carta de los Derechos Fundamentales de la Unión Europea. En 2005, las autoridades de protección de datos de los Estados miembros de la Unión Europea y el Supervisor Europeo de Protección de Datos (en lo sucesivo, SEPD) expresaron su firme apoyo a un nuevo instrumento jurídico para la protección de datos personales en el tercer pilar[9]. El Parlamento Europeo recomendó la armonización de las normas existentes en materia de protección de datos personales en los instrumentos del actual «tercer pilar», agrupándolos en un solo instrumento que garantice el mismo nivel de protección de datos que establece el primer pilar[10].

Según el Programa de La Haya, la introducción del principio de disponibilidad depende de condiciones imprescindibles en el ámbito de la protección de datos. Obviamente, el Consejo Europeo reconoció que las disposiciones sobre protección de datos que existen actualmente a nivel europeo no serían suficientes de cara a la aplicación del principio de disponibilidad, que podría incluir modalidades como el acceso recíproco a las bases de datos nacionales o la interoperabilidad de las mismas, o el acceso directo (en línea).

La preocupación por conseguir un nivel suficiente de protección de los datos también se reflejó en un acuerdo de cooperación firmado por siete Estados miembros el 27 de mayo de 2005 en Prüm (Alemania, Austria, Bélgica, Países Bajos, Luxemburgo, Francia y España) y recomendado como modelo para el intercambio de información entre los Estados miembros de la Unión en general. El acuerdo prevé, bajo determinadas condiciones, el acceso automatizado directo de las autoridades represivas de una Parte Contratante a los datos personales en poder de otra Parte Contratante. No obstante, esta forma de cooperación no se aplicará hasta que las disposiciones de protección de datos del acuerdo se hayan transpuesto al Derecho nacional de las Partes.

- **Disposiciones vigentes en el ámbito de la propuesta**

La Carta de los Derechos Fundamentales de la Unión Europea[11] reconoce explícitamente el derecho a la intimidad (artículo 7) y el derecho a la protección de los datos de carácter personal (artículo 8). Estos datos deben tratarse de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recabados que la conciernan y a obtener su rectificación. El respeto de estas normas estará sujeto al control de una autoridad independiente.

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[12] contiene normas esenciales sobre la

---

7 Documento de trabajo del Consejo 6316 /2/01 REV 2 JAI 13.

8 2514ª Reunión del Consejo, Justicia y Asuntos de Interior, Luxemburgo, 5-6 de junio de 2003, documento del Consejo 9845 /03 (Presse 150), p. 32.

9 *Declaration and Position paper on law enforcement and information exchange in the EU*, adoptado por la Conferencia de Primavera de las Autoridades Europeas de Protección de Datos, Cracovia, 25-26 abril de 2005.

10 Nº 1 h) de la Recomendación del Parlamento Europeo destinada al Consejo Europeo y al Consejo sobre el intercambio de información y la cooperación relacionada con delitos de terrorismo [2005/2046(INI)], aprobado el 7 de junio de 2005.

11 DO C 364 de 18.12.2000, p. 1.

12 DO L 281 de 23.11.1995, p. 31.

legitimidad del tratamiento de los datos personales y sobre los derechos del interesado. Incluye disposiciones relativas a los recursos judiciales, la responsabilidad y las sanciones, la transferencia de datos personales a terceros países, códigos de conducta, autoridades específicas de control y un grupo de trabajo, y, por último, normas de ejecución comunitarias. Sin embargo, la Directiva no se aplica a las actividades que quedan fuera del ámbito del Derecho comunitario, como las previstas en el título VI del Tratado de la Unión Europea (TUE). En consecuencia, los propios Estados miembros pueden decidir sobre las normas adecuadas para el tratamiento y la protección de los datos. En el contexto del título VI del TUE, la protección de datos personales se contempla en diversos instrumentos específicos, en particular en instrumentos que establecen sistemas de información comunes a nivel europeo, como: el Convenio de aplicación del Acuerdo de Schengen de 1990, que incluye disposiciones específicas sobre protección de datos aplicables al Sistema de Información de Schengen[13]; el Convenio Europol de 1995[14] y, entre otros, las Normas relativas a la transmisión de datos de carácter personal por Europol a terceros Estados y a terceras instancias[15]; la Decisión de 2002 por la que se crea Eurojust[16] y las Normas del Reglamento interno de Eurojust relativas al tratamiento y a la protección de datos personales[17]; el Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros de 1995, incluidas las disposiciones sobre protección de datos personales aplicables al Sistema de Información Aduanera[18]; y el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea de 2000, en particular su artículo 23[19]. Respecto al Sistema de Información de Schengen, hay que prestar especial atención al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II), sobre el cual la Comisión ya presentó una propuesta de Decisión del Consejo[20] y dos propuestas de Reglamento[21].

Además, hay que tener presente el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y el Convenio nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 1981, su Protocolo Adicional de 2001 relativo a las autoridades de control y los flujos de datos transfronterizos, y la Recomendación nº R (87) 15 de 1987, por la que se regula la utilización de los datos personales en el sector policial. Todos los Estados miembros son partes en el Convenio pero no todos son partes en el Protocolo Adicional.

- **Coherencia con otras políticas y objetivos de la Unión**

Es preciso reconocer las especificidades del tratamiento y la protección de datos en el marco del título VI del Tratado de la Unión Europea. Por una parte, no deberían suponer un obstáculo para la coherencia con la política general de la Unión en el ámbito de la protección de la intimidad y la protección de datos sobre la base de la Carta de los Derechos Fundamentales de la Unión Europea y de la Directiva 95/46/CE. Los principios fundamentales de la protección de datos se aplican al tratamiento de los datos en el primer y tercer pilar. Por otra parte, debe garantizarse la coherencia con otros instrumentos que

---

13 DO L 239 de 22.9.2000, p. 19.
14 DO C 316 de 27.11.1995, p. 2.
15 DO C 88 de 30.3.1999, p. 1.
16 DO L 63 de 6.3.2002, p. 1.
17 DO C 68 de 19.3.2005, p. 1.
18 DO C 316 de 27.11.1995, p. 34.
19 DO C 197 de 12.7.2000, pp. 1-15.
20 COM(2005) 230 final.
21 COM(2005) 236 final, COM(2005) 237 final.

establecen obligaciones específicas relacionadas con la información que pudiera ser pertinente para prevenir y combatir la delincuencia. Hay que seguir de cerca la evolución de la situación relativa a la conservación de datos tratados y almacenados en la prestación de servicios públicos de comunicaciones electrónicas o los datos en redes públicas de comunicaciones con fines de prevención, investigación, detección y persecución de la delincuencia y enjuiciamiento de delitos, incluido el terrorismo. Es preciso mencionar la estrecha relación que existe entre la presente propuesta de Decisión marco y la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la conservación de datos tratados en el marco de la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE, presentada por la Comisión[22].

2) CONSULTA DE LAS PARTES INTERESADAS Y EVALUACIÓN DE IMPACTO

- **Consulta de las partes interesadas**

Métodos y principales sectores de consulta, perfil general de los consultados

El 22 de noviembre de 2004 y el 21 de junio de 2005, la Comisión invitó y consultó a expertos de los Gobiernos de los Estados miembros, Islandia, Noruega y Suiza, y el 11 de enero de 2005, a expertos de las autoridades de protección de datos de estos Estados. También estaban representados el SEPD, Europol, Eurojust y la Secretaría de las Autoridades comunes de control. La principal finalidad de las consultas era averiguar si era necesario disponer de un instrumento jurídico en relación con el tratamiento y la protección de datos personales en el tercer pilar y, en caso afirmativo, cuál debería ser su contenido principal. La Comisión preguntó a las partes interesadas, sobre la base de un cuestionario y de un documento de debate, su posición respecto al enfoque general de un nuevo instrumento jurídico y su relación con los instrumentos existentes, la base jurídica, el posible ámbito de aplicación, los principios relativos a la calidad de los datos, los criterios para legitimar el tratamiento de los datos por las autoridades policiales o judiciales, datos personales de personas no sospechosas, los requisitos para la transmisión de datos personales a las autoridades competentes de otros Estados miembros y de terceros países, los derechos del interesado, las autoridades de control y un posible organismo consultivo para la protección de datos en el tercer pilar.

Se informó regularmente al Grupo creado en virtud del artículo 29 de la Directiva 95/46/CE sobre los progresos de las consultas. El 12 de abril y el 21 de junio de 2005, la Comisión asistió a reuniones del Grupo de trabajo «Policía» de la Conferencia de las autoridades europeas de protección de datos. El 31 de enero de 2005, la Comisión participó en el «Seminario público: Protección de datos y seguridad de los ciudadanos: ¿qué principios para la Unión Europea?» celebrado por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior. La Comisión tuvo en cuenta los resultados de la Conferencia de Primavera de las Autoridades Europeas de Protección de Datos, celebrada en Cracovia los días 25 y 26 de abril de 2005, y la posición del Parlamento Europeo expuesta, por ejemplo, en la Recomendación del Parlamento Europeo destinada al Consejo Europeo y al Consejo sobre el intercambio de información y la cooperación relacionada con delitos de terrorismo [2005/2046(INI)], aprobada el 7 de junio de 2005.

Resumen de las respuestas y forma en que se han tenido en cuenta

Tanto el Parlamento Europeo como las autoridades de protección de datos de la Unión Europea apoyan decididamente un instrumento jurídico sobre protección de datos personales

[22] COM(2005) 438 final de 21.9.2005.

en el tercer pilar. Representantes de los Gobiernos de los Estados miembros, de Islandia, Noruega y Suiza, y de Europol y Eurojust no expresaron una posición común a este respecto. Sin embargo, la Comisión pudo concluir que no existía una oposición importante a la idea de un instrumento de este tipo. Parece haber acuerdo sobre la necesidad de que la aplicación del principio de disponibilidad vaya acompañada de normas de compensación adecuadas en el ámbito de la protección de datos. Algunos Estados miembros declararon que primero deberían definirse las modalidades de intercambio de información en el futuro y, posteriormente, establecerse las normas para la protección de los datos personales. Otros manifestaron su preferencia por incluir un conjunto de disposiciones específicas en el acto relativo al principio de disponibilidad.

Habiendo sopesado las diversas posiciones, la Comisión es de la opinión de que la aplicación del principio de disponibilidad permitirá desarrollar y modificar radicalmente la calidad e intensidad del intercambio de información entre los Estados miembros. Esta evolución afectará considerablemente a los datos personales y al derecho a la protección de los datos, por lo que debe compensarse debidamente. Iniciativas recientes dirigidas a conseguir un acceso automatizado directo, al menos mediante un sistema de respuesta positiva o negativa, pueden incrementar el riesgo de intercambiar datos ilegítimos, inexactos o no actualizados, y deben tomarse en consideración. Estas iniciativas implican que el responsable del tratamiento ya no podrá verificar *en cada caso individual* la legitimidad de la transmisión y la exactitud de los datos tratados. Por lo tanto, deben ir acompañadas de obligaciones estrictas de garantizar y verificar constantemente la calidad de los datos a los que se autoriza un acceso automatizado directo.

Habida cuenta de la atención prestada al impacto de la aplicación del principio de disponibilidad, las disposiciones que sólo abordan aspectos individuales de la protección de datos no son suficientes. Un instrumento jurídico relativo a la protección de datos personales en el tercer pilar puede, en principio, contribuir a fomentar la cooperación policial y judicial en materia penal, desde el punto de vista de su eficiencia y su legitimidad y del respeto de los derechos fundamentales, en particular el derecho a la protección de los datos personales.

Este instrumento es especialmente necesario con vistas sobre todo a la aplicación del principio de disponibilidad y debe elaborarse paralelamente con la aplicación de este principio. La Decisión marco debe seguir el espíritu y la estructura de la Directiva 95/46/CE en la medida de lo posible, teniendo en cuenta al mismo tiempo las necesidades específicas de la cooperación policial y judicial en materia penal y respetando el principio de proporcionalidad. La Recomendación nº R (87) 15 del Consejo de Europa, de 1987, por la que se regula la utilización de los datos personales en el sector policial, se ha tenido en cuenta para transponer sus principios fundamentales a disposiciones jurídicamente vinculantes a nivel de la UE. Deben establecerse normas claras para la protección de los datos personales que vayan a ponerse o se hayan puesto a disposición de autoridades competentes de otros Estados miembros. Ello implica un sistema que garantice la calidad del tratamiento de los datos en cuestión. Este sistema debe incluir disposiciones que establezcan los derechos pertinentes del interesado y los poderes de las autoridades de control, ya que es probable que el ejercicio de estos derechos y competencias contribuya a la calidad de los datos tratados.

- **Evaluación de impacto**

Se consideraron las siguientes opciones: aplicabilidad de la Directiva 95/46/CE; no presentar propuesta alguna o presentar una propuesta posterior de disposiciones relativas a la protección de datos personales en el tercer pilar; conjunto limitado de disposiciones específicas en un acto jurídico relativo al intercambio de información en el marco del principio de disponibilidad; Decisión marco relativa a la protección de datos personales en el tercer pilar.

Por lo que se refiere a esta última posibilidad, se ha estudiado si un instrumento de esta índole debería aplicarse también al intercambio de datos a través de sistemas de información y por los órganos establecidos a nivel de la UE.

Las disposiciones fundamentales y generales de la Directiva 95/46/CE no son aplicables en el tercer pilar, según lo establecido en su artículo 3, apartado 2. Ni siquiera la supresión de este artículo implicaría automáticamente la aplicabilidad de la Directiva a la cooperación policial y judicial en materia penal. En primer lugar, las especificidades de esta cooperación no se tienen plenamente en cuenta en la Directiva y requerirían una mayor precisión. En segundo lugar, hay que respetar los requisitos de la legislación adoptada en el ámbito del título VI del Tratado de la Unión Europea, cuyo objetivo es fomentar la cooperación policial y judicial en materia penal. Debe excluirse la opción de no presentar ninguna propuesta de disposiciones relativas a la protección de datos personales en el tercer pilar o de presentarla en una fase posterior. Esta opción implicaría probablemente la introducción de nuevas formas de intercambio de información con la aplicación del principio de disponibilidad, sin garantizar una observancia estricta de condiciones imprescindibles en el ámbito de la protección de datos. Un conjunto limitado de disposiciones específicas en un acto jurídico relativo al intercambio de información en el marco del principio de disponibilidad no es suficiente, habida cuenta del impacto probable de este último. Así pues, la única opción plenamente satisfactoria es una Decisión marco relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. Para los Estados miembros esta opción probablemente representará gastos administrativos mínimos o nulos.

La Comisión llevó a cabo una evaluación de impacto, que figura en el Programa de trabajo, y el informe correspondiente puede consultarse en la siguiente dirección: http://europa.eu.int/comm/dgs/justice_home/evaluation/dg_coordination_evaluation_annexe_en.htm.

3) ASPECTOS JURÍDICOS DE LA PROPUESTA

- **Resumen de la acción propuesta**

La propuesta de Decisión marco incluye normas generales sobre la legalidad del tratamiento de datos personales, disposiciones relativas a formas específicas de tratamiento (puesta a disposición o transmisión de datos personales a las autoridades competentes de otros Estados miembros, tratamiento posterior, en particular transmisión posterior, de datos enviados o puestos a disposición por las autoridades competentes de otros Estados miembros), los derechos del interesado, la confidencialidad y la seguridad del tratamiento, los recursos judiciales, la responsabilidad, las sanciones, la autoridad de control y un grupo de protección de las personas en lo que respecta al tratamiento de datos personales con fines de prevención, investigación, detección y enjuiciamiento de delitos. Debe prestarse una atención particular al principio según el cual los datos personales solamente se transferirán a terceros países y organismos internacionales que garanticen un nivel adecuado de protección. La Decisión marco prevé un mecanismo que permite respetar este principio a escala de la UE.

- **Base jurídica**

La presente Decisión marco se basará en los artículos 30 y 31 y en el artículo 34, apartado 2, letra b), del Tratado de la Unión Europea. Habida cuenta en particular de la aplicación del principio de disponibilidad, es esencial contar con disposiciones adecuadas para el tratamiento y la protección de datos personales, incluidas normas comunes para la transmisión de estos datos a terceros países y a organismos internacionales, con el fin de mejorar la cooperación policial y judicial en materia penal, sobre todo en la lucha contra el terrorismo y los delitos

graves. Por otra parte, la confianza mutua entre los Estados miembros sólo será posible si se establecen normas claras y comunes para una eventual transmisión posterior de los datos intercambiados, en especial a terceros países. Las disposiciones propuestas garantizarán que el intercambio de información entre las autoridades competentes no se vea perjudicado por la existencia de diferentes niveles de protección de datos en los Estados miembros.

- **Principios de subsidiariedad y proporcionalidad**

La presente Decisión marco aborda situaciones de especial relevancia para la cooperación policial y judicial en materia penal entre los Estados miembros, en particular para el intercambio de información, con el fin de garantizar e impulsar medidas eficaces y legítimas para prevenir y combatir la delincuencia, sobre todo los delitos graves y el terrorismo, en todos los Estados miembros. Las soluciones nacionales, bilaterales o multilaterales pueden ser útiles para los Estados miembros individualmente, pero desatenderían la necesidad de garantizar la seguridad interna en toda la Unión. Las necesidades de información de las autoridades represivas dependen en gran medida del nivel de integración entre los países. En el marco de la represión de actividades ilícitas, cabe prever un incremento de los intercambios de información entre los Estados miembros, y ello debe ir acompañado de normas coherentes en materia de tratamiento y protección de datos. La presente Decisión marco respeta el principio de subsidiariedad previsto en el artículo 2 del Tratado de la Unión Europea y el artículo 5 del Tratado constitutivo de la Comunidad Europea, en la medida en que pretende aproximar disposiciones legales y reglamentarias de los Estados miembros, objetivo que no podría cumplirse adecuadamente si los Estados miembros actúan de forma unilateral y que requiere una acción concertada en la Unión Europea. De conformidad con el principio de proporcionalidad enunciado en este último artículo, la presente Decisión no excede de lo necesario para alcanzar estos objetivos. En particular, la presente Decisión se refiere únicamente al tratamiento de datos personales en la medida en que resulta pertinente para la cooperación policial y judicial en materia penal.

- **Instrumentos elegidos**

Instrumento propuesto: Decisión marco. El objetivo del presente instrumento jurídico es la aproximación de las disposiciones legales y reglamentarias de los Estados miembros relativas a la protección de datos personales tratados con el fin de prevenir y combatir la delincuencia.

4) REPERCUSIONES PRESUPUESTARIAS

La aplicación de la Decisión marco propuesta implicaría únicamente gastos administrativos suplementarios mínimos, con cargo al presupuesto de las Comunidades Europeas, para las reuniones y los servicios de secretaría del Comité y el grupo consultivo que deben crearse en virtud de los artículos 16 y 31.

2005/0202 (CNS)

Propuesta de

DECISIÓN MARCO DEL CONSEJO

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,[23]

Visto el dictamen del Parlamento Europeo,[24]

Considerando lo siguiente:

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

(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, implica la necesidad de tratar información pertinente con sujeción a las disposiciones correspondientes relativas a la protección de datos personales.

(3) La legislación perteneciente al ámbito del título VI del Tratado de la Unión Europea debería estimular la cooperación policial y judicial en materia penal desde el punto de vista de su eficacia y su legitimidad y del cumplimiento de derechos fundamentales, en particular el derecho a la intimidad y a la protección de datos personales. La existencia de normas comunes relativas al tratamiento y la protección de datos personales tratados con el fin de prevenir y luchar contra la delincuencia puede contribuir 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 imprescindibles en el ámbito de la protección de datos, e invitaba a la Comisión a presentar propuestas a este respecto para finales de 2005. Ello se plasmó en el *Plan de Acción del Consejo y de 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*[25].

---

23 …

24 …

25 DO C 198 de 12.8.2005, p. 1.

(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, debería basarse en normas vinculantes claras que refuercen la confianza mutua entre las autoridades competentes y garanticen la protección de la información pertinente de una forma que quede excluido cualquier obstáculo a esta cooperación entre los Estados miembros y al mismo tiempo se respeten plenamente los derechos individuales fundamentales. Los instrumentos existentes a nivel europeo 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[26], no es aplicable al tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por el título VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento que afecte a la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal.

(6) Un instrumento jurídico que establezca normas comunes para la protección de datos personales tratados con el fin de prevenir y luchar contra la delincuencia debería ser coherente con la política general de la Unión Europea en el ámbito de la protección de la intimidad y de la protección de datos. Siempre que sea posible, teniendo en cuenta la necesidad de mejorar la eficacia de las actividades legítimas de las autoridades policiales, aduaneras, judiciales y otras autoridades competentes, este instrumento debería por tanto atenerse a definiciones y principios existentes y reconocidos, especialmente los de la Directiva 95/46/CE del Parlamento Europeo y del Consejo o los relativos al intercambio de información por Europol, Eurojust, o a su tratamiento dentro del Sistema de Información Aduanera u otros instrumentos comparables.

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

(8) Es necesario especificar los objetivos de la protección de datos en el marco de las actividades policiales y judiciales y establecer normas referentes a la legalidad del tratamiento de datos personales, con el fin de garantizar que cualquier información que pudiera intercambiarse se haya tratado legítimamente y de conformidad con principios fundamentales relativos a la calidad de los datos. Al mismo tiempo, no deberían verse comprometidas en modo alguno las actividades legítimas de las autoridades policiales, aduaneras, judiciales y otras autoridades competentes.

(9) Garantizar un nivel elevado de protección de los datos personales de los ciudadanos europeos requiere disposiciones comunes para determinar la legalidad y la calidad de los datos tratados por las autoridades competentes de otros Estados miembros.

(10) Conviene definir a nivel europeo las condiciones en las que debería autorizarse a las autoridades competentes de los Estados miembros a poner a disposición o transmitir datos personales a autoridades y particulares de otros Estados miembros.

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

---

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

(12) Cuando los datos personales se transfieran de un Estado miembro de la Unión Europea a terceros países o a organismos internacionales, estos datos deberían, en principio, gozar de un nivel de protección adecuado.

(13) La presente Decisión marco debería definir el procedimiento de adopción de las medidas necesarias para evaluar el nivel de protección de datos en un tercer país o en un organismo internacional.

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

(15) Conviene establecer normas comunes sobre confidencialidad y seguridad del tratamiento, responsabilidad y sanciones por utilización ilícita por las autoridades competentes, y sobre recursos judiciales a disposición del interesado. Por otro lado, es necesario que los Estados miembros prevean sanciones penales para las infracciones especialmente graves e intencionadas de las disposiciones relativas a la protección de datos.

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

(17) Estas autoridades deberían disponer de los medios necesarios para cumplir sus funciones, entre ellos poderes de investigación y de intervención, en particular en casos de reclamaciones presentadas por particulares, o capacidad de incoar un procedimiento. Deberían contribuir a garantizar la transparencia de los tratamientos de datos efectuados en los Estados miembros de los que dependan. Sin embargo, sus competencias no deberían afectar a las normas específicas previstas para los procedimientos penales ni a la independencia del poder judicial.

(18) Debería crearse un grupo de protección de las personas en lo que respecta al tratamiento de datos personales con fines de prevención, investigación, detección y enjuiciamiento de delitos, que ejercería sus funciones con plena independencia. Tendría por cometido asesorar a la Comisión y a los Estados miembros y contribuir, en particular, a la aplicación uniforme de las normas nacionales adoptadas en aplicación de la presente Decisión marco.

(19) 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 modifiquen o completen. 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 del Parlamento Europeo y del Consejo, 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[27], y 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

[27] DO L 8 de 12.1.2001, p. 1.

en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)[28].

(20) La presente Decisión marco se entenderá sin perjuicio de las disposiciones específicas en materia de protección de datos establecidas en los instrumentos jurídicos pertinentes relativos al tratamiento y la protección de datos personales por Europol, Eurojust y el Sistema de Información Aduanera.

(21) Las disposiciones relativas a la protección de los datos personales, previstas en el título IV del Convenio de 1990 de aplicación del Acuerdo de Schengen de 14 de junio de 1985 relativo a la supresión gradual de los controles en las fronteras comunes[29] (denominado en lo sucesivo el «Convenio de Schengen») e integrado en el marco de la Unión Europea en virtud del Protocolo anejo al Tratado de la Unión Europea y al Tratado constitutivo de la Comunidad Europea, deberían ser sustituidas por las normas de la presente Decisión marco con respecto a las materias que entran en el ámbito de aplicación del Tratado UE.

(22) Conviene que la presente Decisión marco se aplique a los datos personales tratados en el contexto del Sistema de Información de Schengen de segunda generación y al intercambio correspondiente de información complementaria en aplicación de la Decisión JAI/2006/.... relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación.

(23) La presente Decisión marco se entenderá sin perjuicio de las normas aplicables al acceso ilegal a los datos, previstas en la Decisión marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información[30].

(24) Conviene sustituir el artículo 23 del Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea[31].

(25) Cualquier referencia al Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales debería entenderse como referencia a la presente Decisión marco.

(26) Puesto que los objetivos de la acción que va a llevarse a cabo, 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 lograrlos los Estados miembros de manera suficiente si actúan solos y que, por consiguiente, debido a la dimensión y los efectos de la acción, pueden lograrse mejor a nivel de la Unión Europea, el Consejo puede adoptar medidas con arreglo al principio de subsidiariedad enunciado en el artículo 5 del Tratado CE y mencionado en el artículo 2 del Tratado UE. De conformidad con el principio de proporcionalidad enunciado en el artículo 5 del Tratado CE, la presente Decisión marco no excede de lo necesario para alcanzar esos objetivos.

(27) El Reino Unido participa en la presente Decisión marco, 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 con el artículo 8, apartado 2, de la Decisión 2000/365/CE del

---

28 DO L 201 de 31.7.2001, p. 37.
29 DO L 239 de 22.9.2000, p. 19.
30 DO L 69 de 16.3.2005, p. 67.
31 DO C 197 de 12.7.2000, p. 3.

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 [32].

(28) Irlanda participa en la presente Decisión marco, 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 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;

(29) 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, que entran en el ámbito mencionado en el artículo 1, punto H, de la Decisión 1999/437/CE del Consejo, de 17 de mayo de 1999, relativa a determinadas normas de desarrollo de dicho Acuerdo[33].

(30) Por lo que se refiere a Suiza, la presente Decisión marco desarrolla disposiciones del acervo de Schengen, en el sentido del Acuerdo 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, que entran en el ámbito mencionado en el artículo 1, punto H, de la Decisión 1999/437/CE del Consejo, de 17 de mayo de 1999, relativa a determinadas normas de desarrollo de dicho Acuerdo, leído en conjunción con el artículo 4, apartado 1, de la Decisión 2004/849/CE del Consejo relativa a la firma, en nombre de la Unión Europea, y a la aplicación provisional de determinadas disposiciones de dicho Acuerdo[34].

(31) La presente Decisión marco constituye un acto que desarrolla el acervo de Schengen o está relacionado con él de otro modo en el sentido del artículo 3, apartado 1, del Acta de Adhesión de 2003.

(32) 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. La presente Decisión marco pretende garantizar el pleno respeto de los derechos a la vida privada y a la protección de los datos de carácter personal previstos en los articulos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

HA ADOPTADO LA PRESENTE DECISIÓN MARCO:

CAPÍTULO I
OBJETO, DEFINICIONES Y ÁMBITO DE APLICACIÓN

Artículo 1
Objeto

1. La presente Decisión marco determina normas comunes para garantizar la protección de las personas en lo que respecta al tratamiento de datos personales en el marco de

---

32 DO L 131 de 1.6.2000, p. 43.
33 DO L 176 de 10.7.1999, p. 31.
34 DO L 368 de 15.12.2004, p. 26.

la cooperación policial y judicial en materia penal, prevista en el título VI del Tratado de la Unión Europea.

2. Los Estados miembros velarán por que la comunicación de datos personales a las autoridades competentes de otros Estados miembros no quede restringida ni prohibida por motivos vinculados a la protección de datos personales de conformidad con 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 a 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» («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) «fichero de datos personales» («fichero»): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

d) «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; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas nacionales o por legislación adoptada de conformidad con el título VI del Tratado de la Unión Europea, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o por la legislación adoptada de conformidad con el título VI del Tratado de la Unión Europea;

e) «encargado del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento;

f) «tercero»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento;

g) «destinatario»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero;

h) «consentimiento del interesado»: toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan;

i) «organismos internacionales»: organismos u organizaciones establecidos mediante acuerdos internacionales;

j) «autoridades competentes»: cuerpos de policía, autoridades judiciales, aduaneras y otras autoridades competentes de los Estados miembros en el sentido del artículo 29 del Tratado de la Unión Europea.

Artículo 3
Ámbito de aplicación

1. La presente Decisión marco se aplicará al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero por una autoridad competente, con fines de prevención, investigación, detección o enjuiciamiento de delitos.

2. Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales por:

– la Oficina Europea de Policía (Europol),

– la Unidad Europea de Cooperación Judicial (Eurojust),

– el Sistema de Información Aduanera, establecido con arreglo al Convenio elaborado sobre la base del artículo K.3 del Tratado de la Unión Europea, relativo a la utilización de la tecnología de la información a efectos aduaneros, y las modificaciones correspondientes.

CAPÍTULO II
NORMAS GENERALES SOBRE LA LEGALIDAD DEL TRATAMIENTO DE DATOS PERSONALES

Artículo 4
Principios relativos a la calidad de los datos

1. Los Estados miembros dispondrán que los datos personales sean:

a) tratados de manera leal y lícita;

b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas;

c) adecuados, pertinentes y no excesivos en relación con los fines para los que se hubieran recabado o para los que se traten posteriormente;

d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que se hubieran recogido o para los que se traten posteriormente, sean suprimidos o rectificados; los Estados miembros podrán prever el tratamiento de datos con niveles distintos de precisión y fiabilidad, en cuyo caso deberán disponer que los datos se clasifiquen según su grado de

exactitud y fiabilidad, y que los datos basados en hechos se distingan de los basados en opiniones o apreciaciones personales;

e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán garantías adecuadas para los datos personales conservados durante un período más largo del mencionado con fines históricos, estadísticos o científicos.

2. Corresponderá al responsable del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1.

3. Los Estados miembros establecerán la obligación de distinguir claramente entre datos personales relativos a

- una persona sospechosa de haber cometido o participado en un delito,
- una persona que haya sido objeto de una condena penal,
- una persona de la que se sospeche fundadamente que cometerá un delito,
- una persona que pueda ser citada para testificar en investigaciones relacionadas con delitos o en ulteriores procedimientos penales,
- una persona que haya sido víctima de un delito o respecto de la cual existan sospechas fundadas de que podría serlo,
- una persona que pueda proporcionar información sobre delitos,
- una persona con la que alguna de las personas mencionadas anteriormente haya estado en contacto o asociada, y
- una persona que no pertenezca a ninguna de las categorías mencionadas anteriormente.

4. Los Estados miembros dispondrán que el tratamiento de datos personales sólo sea necesario si

- existen, sobre la base de hechos probados, motivos razonables para creer que los datos personales en cuestión permitirían, facilitarían o acelerarían la prevención, la investigación, la detección o el enjuiciamiento de un delito, y
- no existe ningún otro medio que afecte en menor medida al interesado y
- el tratamiento de los datos no es excesivo en relación con el delito de que se trate.

Artículo 5
Criterios para legitimar el tratamiento de datos

Los Estados miembros dispondrán que los datos personales únicamente puedan ser tratados por las autoridades competentes en virtud de una ley que establezca que el tratamiento es necesario para el cumplimiento de las funciones legales de la autoridad en cuestión y con fines de prevención, investigación, detección y enjuiciamiento de delitos.

Artículo 6
Tratamiento de categorías especiales de datos

1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o

filosóficas, y la afiliación sindical, así como el tratamiento de los datos relativos a la salud o a la vida sexual.

2. Lo dispuesto en el apartado 1 no se aplicará si:

– el tratamiento está previsto por una ley y es absolutamente necesario para el ejercicio de las funciones legales de la autoridad en cuestión, con el fin de prevenir, investigar, detectar y enjuiciar delitos o si el interesado ha dado su consentimiento explícito a dicho tratamiento, y

– los Estados miembros establecen garantías específicas adecuadas, por ejemplo limitar el acceso a los datos en cuestión al personal responsable de ejercer las funciones legales que justifican el tratamiento.

Artículo 7
Plazos para la conservación de datos personales

1. Los Estados miembros dispondrán que los datos se conserven durante un período no superior al necesario para los fines para los que hubieran sido recogidos, salvo que la legislación nacional disponga otra cosa. Los datos personales de las personas a que se refiere el artículo 4, apartado 3, último guión, se conservarán únicamente durante el período que sea absolutamente necesario para la finalidad para la que fueron recogidos.

2. Los Estados miembros establecerán medidas procesales y técnicas adecuadas que garanticen la observancia de los plazos de conservación de datos personales. Se revisará regularmente el cumplimiento de estos plazos.

CAPÍTULO III - Formas específicas de tratamiento

SECCIÓN I - PUESTA A DISPOSICIÓN Y TRANSMISIÓN DE DATOS PERSONALES A LAS AUTORIDADES COMPETENTES DE OTROS ESTADOS MIEMBROS

Artículo 8
Puesta a disposición y transmisión de datos personales a las autoridades competentes de otros Estados miembros

Los Estados miembros dispondrán que los datos personales solamente se transmitan o se pongan a disposición de las autoridades competentes de otros Estados miembros en caso necesario para el cumplimiento de las funciones legales de la autoridad que los transmite o que los recibe y con fines de prevención, investigación, detección o enjuiciamiento de delitos.

Artículo 9
Control de la calidad de los datos transmitidos o puestos a disposición

1. Los Estados miembros dispondrán que la calidad de los datos personales se controle a más tardar antes de su transmisión o puesta a disposición. En la medida de lo posible, las resoluciones judiciales y las resoluciones de sobreseimiento deberán mencionarse en todas las transmisiones de datos y, antes de ser comunicados, deberán verificarse en la fuente los datos basados en opiniones o apreciaciones personales e indicarse su nivel de exactitud o fiabilidad.

2. Los Estados miembros dispondrán que se controle periódicamente la calidad de los datos personales que se pongan a disposición de las autoridades competentes de otros Estados miembros mediante acceso automatizado directo, con el fin de garantizar que se accede a datos exactos y actualizados.

3. Los Estados miembros dispondrán que los datos personales que ya no sean exactos o actualizados no se transmitan ni se pongan a disposición.

4. Los Estados miembros establecerán la obligación de la autoridad competente que haya puesto a disposición o transmitido datos personales a una autoridad competente de otro Estado miembro de informar inmediatamente a esta última si comprueba, por iniciativa propia o a instancias del interesado, que los datos en cuestión no deberían haberse transmitido o puesto a disposición, o que se han transmitido o puesto a disposición datos inexactos u obsoletos.

5. Los Estados miembros establecerán la obligación de la autoridad competente a la que se haya informado de conformidad con el apartado 4 de suprimir o rectificar los datos de que se trate. Además, dicha autoridad rectificará dichos datos si descubre que son inexactos. Si la autoridad tiene motivos fundados para pensar que los datos personales recibidos son inexactos o deben suprimirse, informará sin demora a la autoridad competente que transmitió o puso a disposición dichos datos.

6. Los Estados miembros dispondrán, sin perjuicio de los procedimientos penales nacionales, que se marquen los datos personales a petición del interesado si éste niega que sean exactos y si no puede verificarse su exactitud o inexactitud. Esta marca se suprimirá únicamente con el consentimiento del interesado o sobre la base de una resolución del órgano jurisdiccional competente o de la autoridad de control competente.

7. Los Estados miembros dispondrán que se supriman los datos personales enviados por la autoridad de otro Estado miembro

   – si estos datos no deberían haberse transmitido, puesto a disposición o recibido;

   – cuando expire el plazo que fija la ley del otro Estado miembro si la autoridad que ha transmitido o puesto a disposición los datos en cuestión hubiera comunicado a la autoridad destinataria dicho plazo en el momento de transmitir o poner a disposición los datos, a menos que los datos personales sigan siendo necesarios para procedimientos judiciales;

   – si estos datos no son o han dejado de ser necesarios para los fines para los que se transmitieron o se pusieron a disposición.

8. Si se hubieran transmitido datos personales sin haberlos solicitado previamente, la autoridad destinataria verificará sin demora si estos datos son necesarios para el fin para el cual se transmitieron.

9. Los datos personales no se suprimirán sino que se bloquearán de conformidad con el Derecho nacional si existen motivos razonables para creer que la supresión podría afectar a intereses del interesado dignos de protección. Los datos bloqueados solamente se utilizarán o se transmitirán para la finalidad para la que no se hayan suprimido.

Artículo 10
Registro y documentación

1. Los Estados miembros dispondrán que se registre cada transmisión y recepción automatizadas de datos personales, en particular mediante acceso automatizado directo, para permitir la verificación posterior de los motivos de la transmisión, los datos transmitidos, el momento de la transmisión, las autoridades implicadas y, por lo que a la autoridad destinataria se refiere, las personas que hayan recibido los datos y que hayan dado lugar a su recepción.

2. Los Estados miembros dispondrán que se documente cada transmisión y recepción no automatizadas de datos personales para permitir la verificación posterior de los motivos de la transmisión, los datos transmitidos, el momento de la transmisión, las autoridades implicadas y, por lo que a la autoridad destinataria se refiere, las personas que hayan recibido los datos y que hayan dado lugar a su recepción.

3. La autoridad que haya registrado o documentado esta información la comunicará sin demora a la autoridad de control competente que la solicite. La información solamente se utilizará para el control de la protección de datos y para garantizar su tratamiento adecuado, así como su integridad y seguridad.

SECCIÓN II – TRATAMIENTO POSTERIOR, EN PARTICULAR TRANSMISIÓN Y TRANSFERENCIA POSTERIORES, DE DATOS ENVIADOS O PUESTOS A DISPOSICIÓN POR AUTORIDADES COMPETENTES DE OTROS ESTADOS MIEMBROS

Artículo 11
Tratamiento posterior de datos personales enviados o puestos a disposición por la autoridad competente de otro Estado miembro

1. Los Estados miembros dispondrán que los datos personales enviados o puestos a disposición por la autoridad competente de otro Estado miembro solamente sean objeto de tratamiento posterior, de conformidad con la presente Decisión marco, en particular sus artículos 4, 5 y 6,

   a) para la finalidad específica para la que se transmitieron o pusieron a disposición o

   b) en caso necesario, con fines de prevención, investigación, detección o enjuiciamiento de delitos o con fines de prevención de amenazas para la seguridad pública o para una persona, salvo cuando prevalezca la necesidad de proteger los intereses o los derechos fundamentales del interesado.

2. Los datos personales de que se trate sólo serán objeto de un tratamiento posterior para los fines mencionados en el apartado 1, letra b), del presente artículo con el consentimiento previo de la autoridad que transmitió o puso a disposición los datos personales.

3. El apartado 1, letra b), no será aplicable si una legislación específica en el marco del título VI del Tratado de la Unión Europea dispone explícitamente que los datos personales enviados o puestos a disposición por la autoridad competente de otro Estado miembro solamente serán objeto de tratamiento posterior para los fines para los que se transmitieron o se pusieron a disposición.

Artículo 12
Transmisión a otras autoridades competentes

Los Estados miembros dispondrán que los datos personales enviados o puestos a disposición por la autoridad competente de otro Estado miembro se pongan a disposición o se transmitan ulteriormente a otras autoridades competentes de un Estado miembro solamente si se cumplen todos los requisitos siguientes:

a) la transmisión o puesta a disposición es objeto de una obligación o autorización legal clara;

b) la transmisión o puesta a disposición es necesaria para el cumplimiento de las funciones legales de la autoridad que ha recibido los datos en cuestión o de la autoridad a la que se transmitirán ulteriormente;

c) la transmisión o puesta a disposición es necesaria para la finalidad específica para la que se transmitieron o se pusieron a disposición, o con fines de prevención, investigación, detección o enjuiciamiento de delitos, o con fines de prevención de amenazas para la seguridad pública o para una persona, salvo cuando prevalezca la necesidad de proteger los intereses o los derechos fundamentales del interesado;

d) la autoridad competente del Estado miembro que ha puesto a disposición o transmitido los datos en cuestión a la autoridad competente que se propone a su vez transmitirlos o ponerlos a disposición ha dado su consentimiento a la transmisión o puesta a disposición posterior.

Artículo 13
Transmisión a autoridades distintas de las autoridades competentes

Los Estados miembros dispondrán que los datos personales enviados o puestos a disposición por la autoridad competente de otro Estado miembro se transmitan posteriormente a autoridades distintas de las autoridades competentes de un Estado miembro solamente en determinados casos y si se cumplen todos los requisitos siguientes:

a) la transmisión es objeto de una obligación o autorización legal clara y

b) la transmisión es

necesaria para el fin específico para el que se transmitieron o se pusieron a disposición los datos, o con fines de prevención, investigación, detección o enjuiciamiento de delitos, o con fines de prevención de amenazas para la seguridad pública o para una persona, salvo cuando prevalezca la necesidad de proteger los intereses o los derechos fundamentales del interesado;

o

necesaria porque los datos en cuestión son imprescindibles para que la autoridad a la que se transmitirán posteriormente pueda ejercer sus funciones legales y a condición de que la finalidad de la recogida o el tratamiento que debe llevar a cabo dicha autoridad no sea incompatible con el tratamiento original previsto, y las obligaciones legales de la autoridad competente que se propone transmitir los datos no se opongan a ello,

o

no cabe ninguna duda de que la transmisión es en interés de la persona afectada y si ha mediado su consentimiento o las circunstancias permiten deducir sin lugar a equívoco tal consentimiento.

c) La autoridad competente del Estado miembro que ha transmitido o puesto a disposición los datos en cuestión a la autoridad competente que se propone transmitirlos posteriormente ha aceptado esta transmisión ulterior.

Artículo 14
Transmisión a particulares

Los Estados miembros dispondrán, sin perjuicio de las normas nacionales de procedimiento penal, que los datos personales enviados o puestos a disposición por la autoridad competente de otro Estado miembro sólo puedan transmitirse posteriormente a particulares en un Estado miembro en determinados casos y si se cumplen todos los requisitos siguientes:

a) la transmisión es objeto de una obligación o autorización legal clara y

b) la transmisión es necesaria para la finalidad específica para la que se transmitieron o se pusieron a disposición los datos, o con fines de prevención, investigación, detección o enjuiciamiento de delitos o con fines de prevención de amenazas para la seguridad pública, o para una persona, salvo cuando prevalezca la necesidad de proteger los intereses o los derechos fundamentales del interesado, y

c) la autoridad competente del Estado miembro que ha puesto a disposición o transmitido los datos de que se trate a la autoridad competente que se propone transmitirlos posteriormente ha aceptado previamente la transmisión posterior a particulares.

Artículo 15
Transferencia a autoridades competentes de terceros países o a organismos internacionales

1. Los Estados miembros dispondrán que los datos personales enviados o puestos a disposición por la autoridad competente de otro Estado miembro no sean objeto de transferencia posterior a autoridades competentes de terceros países o a organismos internacionales excepto si tal transferencia se atiene a la presente Decisión marco y, además, se cumplen todos los requisitos siguientes:

a) La transferencia es objeto de una obligación o autorización legal clara.

b) La transferencia es necesaria para la finalidad para la que se transmitieron o se pusieron a disposición los datos, o con fines de prevención, investigación, detección o enjuiciamiento de delitos o con fines de prevención de amenazas para la seguridad pública, o para una persona, salvo cuando prevalezca la necesidad de proteger los intereses o los derechos fundamentales del interesado.

c) La autoridad competente del otro Estado miembro que ha puesto a disposición o transmitido los datos de que se trate a la autoridad competente que se propone transmitirlos posteriormente ha aceptado previamente esta transmisión ulterior.

d) El tercer país o el organismo internacional al que se transferirán los datos garantiza un nivel adecuado de protección de los datos.

2. Los Estados miembros garantizarán que el carácter adecuado del nivel de protección que ofrece un tercer país o un organismo internacional se evalúe atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencias. En particular, para la evaluación se tomarán en consideración los siguientes elementos: el tipo de datos, la finalidad y la duración del tratamiento para el que se transfieren los datos, el país de origen y el país de destino final, las normas de Derecho generales y sectoriales vigentes en el tercer país o en el organismo en cuestión, las normas profesionales y las medidas de seguridad en vigor en dichos países, y la existencia de garantías suficientes establecidas por el destinatario de la transferencia.

3. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país o un organismo internacional no garantiza un nivel de protección adecuado con arreglo al apartado 2.

4. Cuando, en el marco del procedimiento previsto en el artículo 16, se compruebe que un tercer país o un organismo internacional no garantiza un nivel de protección adecuado, a tenor del apartado 2, los Estados miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos al tercer país u organismo internacional de que se trate.

5. De conformidad con el procedimiento a que se refiere el artículo 16, podrá declararse que un tercer país o un organismo internacional garantiza un nivel de protección adecuado, a tenor del apartado 2, a la vista de su legislación interna o de los compromisos internacionales que haya suscrito, a efectos de protección de la vida privada o de las libertades y derechos fundamentales de las personas.

6. Excepcionalmente, los datos personales enviados por la autoridad competente de otro Estado miembro podrán transferirse posteriormente a las autoridades competentes de terceros países o a organismos internacionales que no garanticen un nivel adecuado de protección de los datos si resulta absolutamente necesario para proteger intereses esenciales de un Estado miembro o para evitar un peligro grave e inminente que suponga una amenaza para la seguridad pública o para una persona o personas específicas.

Artículo 16
Comité

1. En los casos en que se haga referencia al presente artículo, la Comisión estará asistida por un Comité compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión.

2. El Comité aprobará su reglamento interno a propuesta de su presidente basándose en el reglamento interno estándar publicado en el *Diario Oficial de la Unión Europea*.

3. El representante de la Comisión presentará al Comité un proyecto de medidas. El Comité emitirá su dictamen sobre dicho proyecto en un plazo que el presidente podrá determinar en función de la urgencia de la cuestión de que se trate. El dictamen se emitirá según la mayoría prevista en el artículo 205, apartado 2, del Tratado constitutivo de la Comunidad Europea para las decisiones que el Consejo deba adoptar a propuesta de la Comisión. Los votos de los representantes de los Estados miembros en el seno del Comité se ponderarán del modo establecido en el artículo anteriormente citado. El presidente no votará.

4. La Comisión adoptará las medidas previstas siempre que sean conformes al dictamen del Comité. Si las medidas previstas no son conformes al dictamen del Comité o en caso de ausencia de dictamen, la Comisión presentará sin demora al Consejo una propuesta relativa a las medidas que vayan a adoptarse e informará al Parlamento Europeo.

5. El Consejo podrá pronunciarse sobre la propuesta por mayoría cualificada, dentro de un plazo de dos meses a partir de la fecha en que la propuesta se haya presentado al Consejo.

   Si dentro de ese plazo el Consejo, por mayoría cualificada, manifiesta que se opone a la propuesta, la Comisión la examinará nuevamente. La Comisión podrá presentar al Consejo una propuesta modificada, volver a presentar su propuesta o presentar una propuesta legislativa. Si transcurrido el plazo el Consejo no adopta el acto de ejecución propuesto ni manifiesta su oposición a la propuesta de medidas de ejecución, la Comisión adoptará el acto de ejecución propuesto.

Artículo 17
Excepciones a los artículos 12, 13, 14 y 15

Los artículos 12, 13, 14 y 15 no se aplicarán si una legislación específica adoptada en el marco del título VI del Tratado de la Unión Europea dispone explícitamente que los datos personales enviados o puestos a disposición por la autoridad competente de otro Estado miembro no se transmitirán ulteriormente o sólo se transmitirán si se respetan condiciones más específicas.

Artículo 18
Información a petición de la autoridad competente

Los Estados miembros dispondrán que la autoridad competente que haya enviado o puesto a disposición datos personales sea informada si lo solicita sobre el tratamiento posterior de dichos datos y los resultados logrados.

CAPÍTULO IV
DERECHOS DEL INTERESADO

Artículo 19
Derecho de información en caso de datos recabados del propio interesado con su conocimiento

1. Los Estados miembros dispondrán que el responsable del tratamiento o su representante comunique de forma gratuita a la persona de quien se recaben datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello:

   a) la identidad del responsable del tratamiento y, en su caso, de su representante;

   b) los fines previstos del tratamiento de que van a ser objeto los datos;

   c) cualquier otra información como:

   – la base jurídica del tratamiento,

   – los destinatarios o las categorías de destinatarios de los datos,

   – el carácter obligatorio o voluntario de las respuestas u otras formas de cooperación y las posibles consecuencias de una negativa a responder o a cooperar,

   – la existencia de derechos de acceso y de rectificación de los datos que le conciernen;

   en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

2. La comunicación de la información prevista en el apartado 1 solamente se denegará o se restringirá si es necesario

   a) para permitir al responsable del tratamiento cumplir correctamente sus funciones legales,

   b) para no perjudicar investigaciones, indagaciones o procedimientos en curso, o el cumplimiento de las funciones legales de las autoridades competentes,

   c) para proteger la seguridad pública y el orden público en un Estado miembro,

   d) para proteger los derechos y libertades de terceros,

   salvo cuando prevalezca la necesidad de proteger los intereses o los derechos fundamentales del interesado.

3. Si la información a que se refiere el apartado 1 se deniega o se restringe, el responsable del tratamiento informará al interesado de su posibilidad de recurrir ante la autoridad de control competente, sin perjuicio de los recursos judiciales existentes y sin perjuicio de los procedimientos penales nacionales.

4. Los motivos de una denegación o restricción con arreglo al apartado 2 no se comunicarán si ello perjudica la finalidad de la denegación. En ese caso, el responsable del tratamiento informará al interesado de su posibilidad de recurrir ante la autoridad de control competente, sin perjuicio de los recursos judiciales existentes y sin perjuicio de los procedimientos penales nacionales. Si el interesado presenta

una reclamación ante la autoridad de control, ésta la examinará. Al estudiar la reclamación, la autoridad de control le informará exclusivamente de si los datos se han tratado de manera correcta y, en caso negativo, de si se ha procedido a las correcciones necesarias.

Artículo 20

Derecho de información cuando los datos no han sido recabados del interesado o han sido recabados del interesado sin su conocimiento

1. En caso de que los datos no se hayan recabado directamente del interesado o se hayan recabado sin su conocimiento o sin que fuera consciente de que se estaban recabando datos que le conciernen, los Estados miembros dispondrán que el responsable del tratamiento o su representante facilite al interesado de forma gratuita, en el momento del registro de los datos personales o, si está prevista una comunicación a un tercero, en un plazo razonable después de la primera comunicación de los datos, al menos la información que se enumera a continuación, salvo si el interesado ya hubiera sido informado de ello o si la comunicación de la información resulta imposible o implicara un esfuerzo desproporcionado:

   a) la identidad del responsable del tratamiento y, en su caso, de su representante;

   b) los fines del tratamiento;

   c) cualquier otra información como:

   – la base jurídica del tratamiento,

   – las categorías de los datos de que se trate,

   – los destinatarios o las categorías de destinatarios de los datos,

   – la existencia de derechos de acceso y rectificación de los datos que le conciernen,

   en la medida en que, habida cuenta de las circunstancias específicas en que se hayan tratado los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

2. La información que debe facilitarse con arreglo al apartado 1 solamente se denegará si es necesario

   a) para permitir al responsable del tratamiento cumplir correctamente sus funciones legales,

   b) para no perjudicar investigaciones, indagaciones o procedimientos en curso, o el cumplimiento de las funciones legales de las autoridades competentes,

   c) para proteger la seguridad pública y el orden público en un Estado miembro,

   d) para proteger los derechos y libertades de terceros,

   salvo cuando prevalezca la necesidad de proteger los intereses o los derechos fundamentales del interesado.

Artículo 21

Derecho de acceso, rectificación, supresión o bloqueo

1. Los Estados miembros garantizarán a todos los interesados el derecho a obtener del responsable del tratamiento:

a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos:

– la confirmación de la existencia o inexistencia de tratamientos de datos que le conciernen, así como información sobre, al menos, los fines del tratamiento, las categorías de datos a que se refiere y los destinatarios o las categorías de destinatarios a quienes se han comunicado dichos datos;

– la comunicación, en forma inteligible, de los datos objeto de tratamiento, así como toda la información disponible sobre el origen de los datos;

b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a lo dispuesto en la presente Decisión marco, en particular cuando tales datos resulten incompletos o inexactos;

c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuados de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado.

2. Las actuaciones a que tiene derecho el interesado de conformidad con el apartado 1 se denegarán si es necesario

a) para permitir al responsable del tratamiento cumplir correctamente sus funciones legales,

b) para no perjudicar investigaciones, indagaciones o procedimientos en curso, o el cumplimiento de las funciones legales de las autoridades competentes,

c) para proteger la seguridad pública y el orden público en un Estado miembro,

d) para proteger los derechos y libertades de terceros,

salvo cuando prevalezca la necesidad de proteger los intereses o los derechos fundamentales del interesado.

3. La denegación o restricción de los derechos a que se refiere el apartado 1 se formulará por escrito. Si el derecho a que se refiere el apartado 1 se deniega o se restringe, el responsable del tratamiento informará al interesado de su posibilidad de recurrir ante la autoridad de control competente, sin perjuicio de los recursos judiciales existentes y sin perjuicio de los procedimientos penales nacionales.

4. Los motivos de una denegación con arreglo al apartado 2 no se comunicarán al interesado si ello perjudica la finalidad de la denegación. En ese caso, el responsable del tratamiento informará al interesado de su posibilidad de recurrir ante la autoridad de control competente, sin perjuicio de los recursos judiciales existentes y sin perjuicio de los procedimientos penales nacionales. Si el interesado presenta una reclamación ante la autoridad de control, ésta la examinará. Al estudiar la reclamación, la autoridad de control le informará exclusivamente de si los datos se han tratado de manera correcta y, en caso negativo, de si se ha procedido a las correcciones necesarias.

Artículo 22
Información a terceros tras la rectificación, el bloqueo o la supresión

Los Estados miembros dispondrán que se tomen las medidas técnicas adecuadas para garantizar que, en caso de que el responsable del tratamiento rectifique, bloquee o suprima datos personales a raíz de una petición en este sentido, se elabore automáticamente una lista

de los proveedores y destinatarios de estos datos. El responsable del tratamiento se asegurará de que las personas incluidas en la lista sean informadas de los cambios introducidos en los datos personales.

CAPÍTULO V
Confidencialidad y seguridad del tratamiento

Artículo 23
Confidencialidad

Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso cuando se lo encargue el responsable del tratamiento, salvo en virtud de un imperativo legal. Todas las personas que deban trabajar con o para una autoridad competente de un Estado miembro estarán sujetas a normas estrictas de confidencialidad.

Artículo 24
Seguridad

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y organizativas adecuadas para la protección de los datos personales contra la destrucción, accidental o ilegal, 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 los mismos mediante acceso automatizado directo, así como contra cualquier otro tipo de tratamiento ilegal de datos personales, 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 del estado de la técnica 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. Una medida se considerará necesaria cuando el esfuerzo que suponga guarde relación con el objetivo de protección que se persiga.

2. Por lo que se refiere al tratamiento automatizado de los 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 por personas no autorizadas (control de los soportes de datos);

   c) impedir que se introduzcan sin autorización en los ficheros, o que puedan conocerse, modificarse o suprimirse sin autorización datos personales almacenados (control del almacenamiento);

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

   e) garantizar que, para el uso de un sistema de tratamiento automatizado de datos, las personas autorizadas sólo puedan tener acceso a los datos que sean de su competencia (control del acceso);

f) garantizar que sea posible verificar y comprobar a qué organismos se han transmitido, pueden transmitirse u ofrecerse datos personales mediante equipos de comunicación de datos (control de las comunicaciones);

g) garantizar que pueda verificarse y comprobarse a posteriori qué datos de carácter personal se han introducido en el sistema de tratamiento automatizado de datos y en qué momento y por qué persona han sido introducidos (control de la introducción);

h) impedir que, en el momento de la transferencia de datos de carácter personal 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 rápidamente en caso de avería (recuperación);

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

3. Los Estados miembros dispondrán que el responsable del tratamiento, en caso de que el tratamiento se efectúe por cuenta del mismo, elija a un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y organizativas que rigen los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.

4. La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:

– que el encargado del tratamiento sólo actuará siguiendo instrucciones del responsable del tratamiento;

– que las obligaciones previstas en los apartados 1 y 2, tal como se definan en la legislación del Estado miembro en el que esté establecido el encargado, incumbirán también a éste.

5. A efectos de conservación de pruebas, los elementos del contrato o del acto jurídico relativo a la protección de datos y los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente.

Artículo 25
Registro

1. Los Estados miembros dispondrán que cada responsable del tratamiento lleve un registro de cada tratamiento o conjunto de tratamientos destinados a la consecución de un fin o de varios fines conexos. El registro deberá contener la siguiente información:

a) el nombre y la dirección del responsable del tratamiento y, en su caso, de su representante;

b) el fin o los fines del tratamiento;

c) una descripción de la categoría o categorías de interesados y de los datos o categorías de datos que les conciernen;

d) la base jurídica del tratamiento al que se destinan los datos;

e) los destinatarios o categorías de destinatarios a los que podrían comunicarse los datos;

f) las transferencias de datos previstas a terceros países;

g) una descripción general que permita evaluar de modo preliminar si las medidas adoptadas en aplicación del artículo 24 resultan adecuadas para garantizar la seguridad del tratamiento.

2. Los Estados miembros especificarán las condiciones y los procedimientos de notificación a la autoridad de control de la información mencionada en el apartado 1.

Artículo 26
Controles previos

1. Los Estados miembros precisarán los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados y velarán por que sean examinados antes de iniciarse el tratamiento.

2. Estos exámenes previos serán realizados por la autoridad de control tras recibir la notificación del responsable del tratamiento o por el encargado de la protección de datos, quien, en caso de duda, deberá consultar a la autoridad de control.

3. Los Estados miembros también podrán proceder a estos exámenes en el curso de la elaboración de una medida legislativa aprobada por el Parlamento nacional o de una medida basada en dicha medida legislativa, que defina la naturaleza del tratamiento y precise las garantías adecuadas.

CAPÍTULO VI
RECURSOS JUDICIALES Y RESPONSABILIDAD

Artículo 27
Vías de recurso

Sin perjuicio de los recursos administrativos que pudieran preverse, en particular ante la autoridad de control mencionada en el artículo 30, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, adoptadas en virtud de la presente Decisión marco.

Artículo 28
Responsabilidad

1. Los Estados miembros dispondrán que toda persona que haya sufrido un perjuicio como consecuencia de un tratamiento ilegal o de un acto incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Decisión marco tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño.

2. No obstante, la autoridad competente que haya recibido datos personales de la autoridad competente de otro Estado miembro será responsable frente a la parte

perjudicada por los daños causados debido a la utilización de datos no actualizados o inexactos. No podrá exonerar su responsabilidad por el hecho de haber recibido datos no actualizados o inexactos de otra autoridad. Si la autoridad destinataria debe pagar una indemnización por daños y perjuicios por el uso de datos incorrectos transmitidos o puestos a disposición por la autoridad competente de otro Estado miembro, ésta última reembolsará íntegramente a la autoridad destinataria el importe de la indemnización por daños y perjuicios.

Artículo 29
Sanciones

1. 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 deberán aplicarse en caso de incumplimiento de las disposiciones adoptadas con arreglo a la presente Decisión marco.

2. Los Estados miembros establecerán sanciones penales eficaces, proporcionadas y disuasorias para las infracciones intencionadas que impliquen una vulneración grave de las disposiciones adoptadas en aplicación de la presente Decisión marco, en particular las disposiciones destinadas a garantizar la seguridad y la confidencialidad del tratamiento.

CAPÍTULO VII
AUTORIDAD DE CONTROL Y GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

Artículo 30
Autoridad de control

1. Cada Estado miembro dispondrá que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros en aplicación de la presente Decisión marco. Estas autoridades ejercerán con total independencia las funciones que les sean atribuidas.

2. Cada Estado miembro dispondrá que se consulte a las autoridades de control en el momento de la elaboración de medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal con fines de prevención, investigación, detección y enjuiciamiento de delitos.

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

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

   – poderes efectivos de intervención, por ejemplo emitir dictámenes antes de realizar los tratamientos, con arreglo al artículo 26, y garantizar una publicación adecuada de dichos dictámenes, ordenar el bloqueo, la supresión o la destrucción de datos, o prohibir provisional o definitivamente un tratamiento, dirigir una advertencia o

amonestación al responsable del tratamiento o recurrir a los Parlamentos nacionales u otras instituciones políticas;

– capacidad de incoar un procedimiento en caso de infracción de las disposiciones nacionales adoptadas con arreglo a la presente Decisión marco o poner dicha infracción en conocimiento de la autoridad judicial.

Las decisiones de la autoridad de control lesivas de derechos son susceptibles de recurso judicial.

4. Toda autoridad de control entenderá de las reclamaciones 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 reclamación.

5. Toda autoridad de control presentará periódicamente un informe sobre sus actividades. Dicho informe será publicado.

6. Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro.

7. Las autoridades de control cooperarán entre sí, así como con las autoridades de control que se creen en el marco del título VI del Tratado de la Unión Europea y con el Supervisor Europeo de Protección de Datos en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de toda información que estimen útil.

8. Los Estados miembros dispondrán que los miembros y agentes de las autoridades de control estarán sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso.

9. Las competencias de la autoridad de control no afectarán a la independencia del poder judicial y las decisiones adoptadas por esta autoridad se aplicarán sin perjuicio de la ejecución de las funciones legales del poder judicial en los procedimientos penales.

Artículo 31

Grupo de protección de las personas en lo que respecta al tratamiento de datos personales con fines de prevención, investigación, detección y enjuiciamiento de delitos

1. Se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales con fines de prevención, investigación, detección y enjuiciamiento de delitos, en lo sucesivo denominado «el Grupo». Este Grupo tendrá carácter consultivo y actuará con independencia.

2. El Grupo estará compuesto por un representante de la autoridad o las autoridades de control designadas por cada Estado miembro, por un representante del Supervisor Europeo de Protección de Datos y por un representante de la Comisión.

Cada miembro del Grupo será designado por la institución, la autoridad o las autoridades a las que represente. Cuando un Estado miembro haya designado varias autoridades de control, éstas nombrarán a un representante común.

Los presidentes de las Autoridades comunes de control creadas en el marco del título VI del Tratado de la Unión Europea tendrán derecho a participar o a estar representados en las reuniones del Grupo. La autoridad o las autoridades de control designadas por Islandia, Noruega y Suiza tendrán derecho a participar en las reuniones del Grupo en la medida en que se aborden cuestiones relacionadas con el acervo de Schengen.

3. El Grupo adoptará sus decisiones por mayoría simple de los representantes de las autoridades de control de los Estados miembros.

4. El Grupo elegirá a su presidente. El mandato del presidente tendrá una duración de dos años. El mandato será renovable.

5. La Comisión asumirá las funciones de secretaría del Grupo.

6. El Grupo aprobará su reglamento interno.

7. El Grupo examinará los asuntos incluidos en el orden del día por su presidente, bien por iniciativa de éste o a solicitud de un representante de las autoridades de control, de la Comisión, del Supervisor Europeo de Protección de Datos o de los presidentes de las Autoridades comunes de control.

Artículo 32

Cometidos

1. El Grupo tendrá por cometido:

   a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales adoptadas en virtud de la presente Decisión marco con vistas a contribuir a su aplicación homogénea;

   b) emitir dictámenes sobre el nivel de protección en los Estados miembros, en terceros países y en organismos internacionales, en particular para garantizar que los datos personales se transfieran de conformidad con el artículo 15 de la presente Decisión marco a terceros países o a organismos internacionales que garanticen un nivel adecuado de protección;

   c) asesorar a la Comisión y a los Estados miembros sobre cualquier propuesta de modificación de la presente Decisión marco, sobre medidas suplementarias o específicas destinadas a proteger los derechos y libertades de las personas físicas por lo que respecta al tratamiento de datos personales con fines de prevención, investigación, detección y enjuiciamiento de delitos, así como cualquier otra medida prevista que afecte a dichos derechos y libertades.

2. Si el Grupo comprobara la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieran afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales en la Unión Europea, informará de ello al Consejo y a la Comisión.

3. El Grupo podrá, por iniciativa propia o a instancias de la Comisión o del Consejo, formular recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de datos personales en la Unión Europea con fines de prevención, investigación, detección y enjuiciamiento de delitos.

4. Los dictámenes y recomendaciones del Grupo se transmitirán al Consejo, a la Comisión, al Parlamento Europeo y al Comité a que se refiere el artículo 16.

5. La Comisión, basándose en la información facilitada por los Estados miembros, informará al Grupo de las medidas tomadas en respuesta a sus dictámenes y recomendaciones. A tal efecto, elaborará un informe, que será transmitido asimismo al Parlamento Europeo y al Consejo. Dicho informe será publicado. Los Estados miembros informarán al Grupo de cualquier medida que adopten con arreglo al apartado 1.

6. El Grupo elaborará un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales con fines de prevención, investigación, detección y enjuiciamiento de delitos en la Unión Europea y en terceros países, y lo transmitirá a la Comisión, al Parlamento Europeo y al Consejo. Dicho informe será publicado.

CAPÍTULO VIII
Disposiciones finales

Artículo 33
Modificación del Convenio de Schengen

A efectos de las materias que entran en el ámbito de aplicación del Tratado UE, la presente Decisión marco sustituye a los artículos 126 a 130 del Convenio de Schengen.

Artículo 34
Relación con otros instrumentos relativos al tratamiento y a la protección de datos personales

1. La presente Decisión marco sustituye al artículo 23 del Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea.

2. Las referencias al Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de los datos personales se entenderán como referencias a la presente Decisión marco.

Artículo 35
Aplicación

1. Los Estados miembros adoptarán las medidas necesarias para cumplir la presente Decisión marco el 31 de diciembre de 2006.

2. 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 sus legislaciones nacionales en virtud de las obligaciones derivadas de la presente Decisión marco, así como información sobre la designación de la autoridad o autoridades de control a que se refiere el artículo 29. Sobre la base de esta información y de un informe escrito de la Comisión, el Consejo evaluará antes del 31 de diciembre de 2007 en qué medida los Estados miembros han adoptado las medidas necesarias para cumplir la presente Decisión marco.

Artículo 36
Entrada en vigor

La presente Decisión marco entrará en vigor el vigésimo día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en Bruselas, el

Por el Consejo
El Presidente

ANEXO

FICHA DE FINANCIACIÓN LEGISLATIVA

Ámbito(s): Justicia e Interior

Actividad(es): 1806 - Establecimiento de un auténtico espacio de libertad, seguridad y justicia en materia civil y penal

TÍTULO DE LA ACCIÓN: PROPUESTA DE DECISIÓN MARCO DEL CONSEJO RELATIVA A LA PROTECCIÓN DE DATOS PERSONALES TRATADOS EN EL MARCO DE LA COOPERACIÓN POLICIAL Y JUDICIAL EN MATERIA PENAL

1. LÍNEA(S) PRESUPUESTARIA(S) + DENOMINACIÓN

ND

2. DATOS GLOBALES EN CIFRAS

2.1. Dotación total de la medida (Parte B): Millones de € en CC

ND

2.2. Periodo de aplicación:

A partir de 2006

2.3. Estimación global plurianual de los gastos:

a) Calendario de créditos de compromiso/créditos de pago (intervención financiera) (*véase el punto 6.1.1*)

en millones de euros (*cifra aproximada al tercer decimal*)

	[2006]	[2007]	[2008]	[2009]	[2010]	[2011]	Total
Compromisos							
Pagos							

b) Asistencia técnica y administrativa (ATA) y gastos de apoyo (GA) (*véase el punto 6.1.2*)

Compromisos							
Pagos							

Subtotal a+b							
Compromisos							
Pagos							

c) Incidencia financiera global de los recursos humanos y otros gastos administrativos *(véanse los puntos 7.2 y 7.3)*

Compromisos/Pagos	0,389	0,389	0,389	0,389	0,389	0,389	2,334

TOTAL a+b+c							
Compromisos							
Pagos							

2.4. Compatibilidad con la programación financiera y las perspectivas financieras

ND

2.5. Incidencia financiera en los ingresos

La propuesta no tiene ninguna incidencia financiera.

3. CARACTERÍSTICAS PRESUPUESTARIAS

Naturaleza del gasto		**Nuevo**	**Contribución AELC**	**Participación de los países candidatos**	**Rúbrica PF**
No obliga-torio	No disoc.	ND	ND	ND	**No** ND

4. BASE JURÍDICA

Artículos 30 y 31 y artículo 34, apartado 2, letra b) del TUE.

5. DESCRIPCIÓN Y JUSTIFICACIÓN

5.1. Necesidad de una intervención comunitaria

5.1.1. Objetivos perseguidos

La Decisión marco propuesta establecerá normas comunes relativas a la protección de datos personales tratados por las autoridades competentes en el contexto de actividades previstas por el título VI del Tratado de la Unión Europea (cooperación policial y judicial en materia penal). Autoridades de control públicas e independientes supervisarán la aplicación de las disposiciones nacionales adoptadas de conformidad con la presente Decisión marco en los Estados miembros. Se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales con fines de prevención, investigación, detección y enjuiciamiento de delitos, en lo sucesivo denominado «el Grupo». El Grupo estará compuesto por un representante de la autoridad o las autoridades de control designadas por cada Estado miembro, por un representante del Supervisor Europeo de Protección de Datos y por un representante de la Comisión. El Grupo estudiará todas las cuestiones relativas a la aplicación de las disposiciones nacionales adoptadas de conformidad con la presente Decisión marco con vistas a contribuir a su aplicación homogénea. Emitirá dictámenes sobre el nivel de protección de datos en los Estados miembros y en terceros países y asesorará a la Comisión y a los Estados miembros sobre cualquier propuesta de modificación de la presente Decisión marco y sobre medidas suplementarias o específicas destinadas a proteger derechos fundamentales.

Además, con arreglo al artículo 16 de la Decisión marco, la Comisión estará asistida por un Comité compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión, con el fin de evaluar, en caso necesario, el nivel de protección de los datos en un tercer país.

5.1.2. Disposiciones adoptadas a raíz de la evaluación ex ante

Se consultó a los representantes de los Gobiernos y de las autoridades independientes de control de los Estados miembros, así como de Islandia, Noruega y Suiza, el Supervisor Europeo de Protección de Datos, Europol y Eurojust. Teniendo en cuenta en particular los diferentes puntos de vista, la Comisión propone la creación del Grupo descrito anteriormente. Para calcular el posible coste que implica la presente medida, la Comisión comprobó los gastos (gastos de viaje y de secretaría para la preparación y organización de reuniones) realizados actualmente por el Grupo establecido de conformidad con el artículo 29 de la Directiva 95/46/CE.

5.2. Acciones previstas y modalidades de intervención presupuestaria

El Grupo previamente mencionado se reunirá probablemente con regularidad: se calcula que cinco veces al año. El Comité mencionado en el artículo 16 se reunirá en caso necesario y siempre que sea necesario, posiblemente también cinco veces al año. Habrá que reembolsar los gastos de un participante por Estado miembro y Estado de Schengen (Islandia, Noruega). Los grupos establecidos de conformidad con los artículos 29 y 31 de la Directiva 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, pueden servir de orientación.

5.3. Métodos de ejecución

La Comisión deberá ser la organizadora y anfitriona de todas las reuniones. La Comisión deberá asumir las tareas de secretaría para el Grupo y el Comité previamente mencionados y preparar/organizar sus reuniones.

6. INCIDENCIA FINANCIERA

6.1. Incidencia financiera total en la Parte B (para todo el período de programación)

6.1.1. Intervención financiera

ND

6.1.2. Asistencia técnica y administrativa (ATA), gastos de apoyo (GA) y gastos de TI (créditos de compromiso)

ND

6.2. Cálculo de los costes por medida prevista en la Parte B (para todo el periodo de programación)

ND

7. INCIDENCIA EN LOS EFECTIVOS Y EN LOS GASTOS ADMINISTRATIVOS

Las necesidades de recursos humanos y administrativos se cubrirán mediante la asignación concedida a la DG responsable en el marco del procedimiento de asignación anual.

La asignación de puestos dependerá también de la atribución de funciones y recursos en el contexto de las perspectivas financieras 2007-2013.

7.1. Incidencia en los recursos humanos

Tipos de puesto		Efectivos a asignar a la gestión de la acción mediante la utilización de recursos existentes y/o suplementarios		Total	Descripción de las tareas que se derivan de la acción
		Número de empleos permanentes	Número de empleos temporales		
Funcionarios o agentes temporales	A B C	0,25 A 0,50 B 1,00 C		0,25A 0,50B 1,00C	Tareas de secretaria, preparación de las reuniones del Grupo y del Comité
Otros recursos humanos					
Total					

7.2. Incidencia financiera global de los recursos humanos

Tipo de recursos humanos	Importe (€)	Método de cálculo*
Funcionarios Agentes temporales	1er año: 189 000	1 X 108 000 0,5 X 108 000 0,25 X 108 000 = 189 000
Otros recursos humanos (indíquese la línea presupuestaria)		
Total	189 000	

Los importes corresponden a los gastos totales de la acción durante 12 meses.

7.3. Otros gastos de funcionamiento que se derivan de la acción

Línea presupuestaria (número y denominación)	Importes en €	Método de cálculo

Dotación global (Título A7) A0701 – Misiones A07030 - Reuniones A07031 - Comités obligatorios A07032- Comités no obligatorios A07040 - Conferencias A0705 - Estudios y consultas Otros gastos (especifíquense)	200 000	10 reuniones * 27 * 740€
Sistemas de información (A-5001/A-4300)		
Otros gastos - Parte A (especifíquense)		
Total	200 000	

Los importes corresponden a los gastos totales de la acción durante 12 meses.

Precisar el tipo de comité, así como el grupo al que pertenece.

I.	Total anual (7.2 + 7.3)	389 000 €
II.	Duración de la acción	
III.	Coste total de la acción (I x II)	

8. SEGUIMIENTO Y EVALUACIÓN

8.1. Sistema de seguimiento

El Grupo y el Comité establecerán su reglamento interno, incluidas las normas de confidencialidad. Se informará al Parlamento Europeo de forma análoga a la establecida en el artículo 7 de la Decisión 99/468/CE del Consejo, de 28 de junio de 1999, por la que se establecen los procedimientos para el ejercicio de las competencias de ejecución atribuidas a la Comisión (DO L 184 de 17.7.1999, p. 23).

8.2. Modalidades y periodicidad de la evaluación prevista

ND

9. MEDIDAS ANTIFRAUDE

ND

XXX