CONVENIO PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL (NÚMERO 108 DEL CONSEJO DE EUROPA), HECHO EN ESTRASBURGO EL 28 DE ENERO DE 1981

(«BOE núm. 274/1985, de 15 de noviembre de 1985»)

Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (número 108 del Consejo de Europa), hecho en Estrasburgo el 28 de enero de 1981.

JUAN CARLOS I REY DE ESPAÑA.

Por cuanto el día 28 de enero de 1982, el Plenipotenciario de España, nombrado en buena y debida forma al efecto, firmó en Estrasburgo el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.

Vistos y examinados los veintisiete artículos del Convenio, Cumplidos los requisitos exigidos por la legislación española, Vengo en aprobar y ratificar cuanto en él se dispone, como en virtud del presente lo apruebo y ratifico, prometiendo cumplirlo, observarlo y hacer que se cumpla y observe puntualmente en todas sus partes, a cuyo fin, para su mayor validación y firmeza, mando expedir este Instrumento de Ratificación firmado por Mí, debidamente sellado y refrendado por el infrascrito Ministro de Asuntos Exteriores.

Dado en Madrid a 27 de enero de 1984.

El Ministro de Asuntos Exteriores, FERNANDO MORAN LOPEZ.

JUAN CARLOS R.

CONVENIO PARA LA PROTECCION DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARACTER PERSONAL.

PREAMBULO.

Los Estados miembros del Consejo de Europa, signatarios del presente Convenio;

Considerando que el fin del Consejo de Europa es llevar a cabo una unión más íntima entre sus miembros, basada en el respeto particularmente de la preeminencia del derecho así como de los derechos humanos y de las libertades fundamentales;

Considerando que es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados;

Reafirmando al mismo tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras;

Reconociendo la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos,

Convienen en lo siguiente:

CAPITULO PRIMERO.
Disposiciones generales.

Artículo 1. Objeto y fin.

El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»).

Artículo 2. Definiciones.

A los efectos del presente Convenio:

a) «datos de carácter personal» significa cualquier información relativa a una persona física identificada o identificable («persona concernida»);

b) «fichero automatizado» significa cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado;

c) por «tratamiento automatizado» se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión;

d) autoridad «controladora del fichero» significa la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán.

Artículo 3. Campo de aplicación.

1. Las Partes se comprometen a aplicar el presente Convenio a los ficheros y a los tratamientos automatizados de datos de carácter personal en los sectores público y privado.

2. Cualquier Estado podrá en el momento de la firma o al depositar su instrumento de ratificación, aceptación, aprobación o adhesión, o en cualquier otro momento ulterior hacer saber mediante declaración dirigida al Secretario general del Consejo de Europa:

a) Que no aplicará el presente Convenio a determinadas categorías de ficheros automáticos de datos de carácter personal, una lista de las cuales quedará depositada. No deberá sin embargo incluir en esa hasta categorías de ficheros automatizados sometidas, con arreglo a su derecho interno, a disposiciones de protección de datos. Deberá, por tanto, modificar dicha lista mediante una nueva declaración cuando estén sometidas a su régimen de protección de datos categorías suplementarias de ficheros automatizados de datos de carácter personal;

b) que aplicará el presente Convenio, asimismo, a informaciones relativas a agrupaciones, asociaciones, fundaciones, sociedades, compañías o cualquier otro organismo compuesto directa o indirectamente de personas físicas, tengan o no personalidad jurídica;

c) que aplicará el presente Convenio, asimismo, a los ficheros de datos de carácter personal que no sean objeto de tratamientos automatizados.

3. Cualquier Estado que haya ampliado el campo de aplicación del presente Convenio mediante una de las declaraciones a que se refieren los apartados 2, b) o c), que anteceden podrá, en dicha declaración, indicar que las ampliaciones solamente se aplicarán a determinadas categorías de ficheros de carácter personal cuya lista quedará depositada.

4. Cualquier Parte que haya excluido determinadas categorías de ficheros automatizados de datos de carácter personal mediante la declaración prevista en el apartado 2, a), anterior no podrá pretender que una Parte que no las haya excluido aplique el presente Convenio a dichas categorías.

5. Igualmente, una Parte que no haya procedido a una u otra de las ampliaciones previstas en los párrafos 2, b) y c), del presente artículo no podrá pretender que se aplique el presente Convenio en esos puntos con respecto a una parte que haya procedido a dichas ampliaciones.

6. Las declaraciones previstas en el párrafo 2 del presente artículo tendrán efecto en el momento de la entrada en vigor del Convenio con respecto al Estado que las haya formulado, si dicho Estado las ha hecho en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, o tres meses después de su recepción por el Secretario general del Consejo de Europa si se han formulado en un momento ulterior. Dichas declaraciones podrán retirarse en su totalidad o en parte mediante notificación dirigida al Secretario general del Consejo de Europa. La retirada tendrá efecto tres meses después de la fecha de recepción de dicha notificación.

CAPITULO II.
Principios básicos para la protección de datos.

Artículo 4. Compromisos de las Partes.

1. Cada Parte tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para

la protección de datos enunciados en el presente capítulo.

2. Dichas medidas deberán adoptarse a más tardar en el momento de la entrada en vigor del presente Convenio con respecto a dicha Parte.

Artículo 5. Calidad de los dalos.

Los datos de carácter personal que sean objeto de un tratamiento automatizado:

a) Se obtendrán y tratarán leal y legítimamente;

b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;

c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;

d) serán exactos y si fuera necesario puestos al día;

e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuates se hayan registrado.

Artículo 6. Categorías particulares de datos.

Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales.

Artículo 7. Seguridad de los datos.

Se tomarán medidas de segundad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

Artículo 8. Garantías complementarias para la persona concernida Cualquier persona deberá poder:

a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero;

b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible;

c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio;

d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo.

Artículo 9. Excepción y restricciones.

1. No se admitirá excepción alguna en las disposiciones de los artículos 5, 6 y 8 del presente Convenio, salvo que sea dentro de los límites que se definen en el presente artículo.

2. Será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presente Convenio cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática:

a) Para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales;

b) para la protección de la persona concernida y de los derechos y libertades de otras personas.

3. Podrán preverse por la ley restricciones en el ejercicio de los derechos a que se refieren los párrafos b), c) y d) del artículo 8 para los ficheros automatizados de datos de carácter personal que se utilicen con fines estadísticos o de

investigación científica, cuando no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas.

Artículo 10. Sanciones y recursos.

Cada Parte se compromete a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos enunciados en el presente capitulo.

Artículo 11. Protección más amplia.

Ninguna de las disposiciones del presente capítulo se interpretará en el sentido de que limite la facultad, o afecte de alguna otra forma a la facultad de cada Parte, de conceder a las personas concernidas una protección más amplia que la prevista en el presente Convenio.

CAPITULO III.
Flujos transfronterizos de Datos.

Artículo 12. Flujos trasfronterizos de datos de carácter personal y el derecho interno.

1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento.

2. Una Parte no podrá, con el único fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte.

3. Sin embargo, cualquier Parte tendrá la facultad de establecer una excepción a las disposiciones del párrafo 2.

a) En la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra Parte establezca una protección equivalente;

b) cuando la transmisión se lleve a cabo a partir de su territorio hacía el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte a que se refiere el comienzo del presente párrafo.

CAPITULO IV.
Ayuda mutua.

Artículo 13. Cooperación entre las Partes.

1. Las Partes se obligan a concederse mutuamente asistencia para el cumplimiento del presente Convenio.

2. A tal fin,

a) cada Parte designará a una o más autoridades cuya denominación y dirección comunicará al Secretario general del Consejo de Europa;

b) cada Parte que haya designado a varias autoridades indicará en la comunicación a, que se refiere el apartado anterior la competencia de cada una de dichas autoridades.

3. Una autoridad designada por una Parte, a petición de una autoridad designada por otra Parte:

a) Facilitará informaciones acerca de su derecho y su práctica administrativa en materia de protección de dalos;

b) tomará toda clase de medidas apropiadas, con arreglo a su derecho interno y solamente a los efectos de la protección de la vida privada, para facilitar informaciones fácticas relativas a un tratamiento automatizado determinado efectuado en su territorio con excepción, sin embargo, de los datos de carácter personal que sean objeto de dicho tratamiento.

Artículo 14. Asistencia a las personas concernidas que tengan su residencia en el extranjero.

1. Cada Parte prestará asistencia a cualquier persona que tenga su residencia en el extranjero para el ejercicio de los derechos previstos por su derecho interno que haga efectivos los principios enunciados en el artículo 8 del presente Convenio.

2. Si dicha persona residiese en el territorio de otra Parte, deberá tener la facultad de presentar su demanda por intermedio de la autoridad designada por esa Parte.

3. La petición de asistencia deberá hacer constar todos los datos necesarios relativos concretamente a:

a) El nombre, la dirección y cualesquiera otros elementos pertinentes de identificación relativos al requirente;

b) el fichero automatizado de datos de carácter personal al que se refiere la demanda o la autoridad controladora de dicho fichero;

c) el objeto de la petición.

Artículo 15. Garantías relativa» a la asistencia facilitada por las autoridades designadas.

1. Una autoridad designada por una Parte que haya recibido información de una autoridad designada por otra Parte, bien en apoyo de una petición de asistencia bien como respuesta a una petición de asistencia que haya formulado ella misma, no podrá nacer uso de dicha información para otros fines que no sean los especificados en la petición de asistencia.

2. Cada parte cuidará de que las personas pertenecientes a la autoridad designada o que actúen en nombre de la misma estén vinculadas por obligaciones convenientes de secreto o de confidencialidad con respecto a dicha información.

3. En ningún caso estará autorizada una autoridad designada para presentar, con arreglo a los términos del artículo 14, párrafo 2, una petición de asistencia en nombre de una persona concernida residente en el extranjero, por su propia iniciativa y sin el consentimiento expreso de dicha persona.

Artículo 16. Denegación de peticiones de asistencia.

Una autoridad designada, a quien se haya dirigido una petición de asistencia con arreglo a los términos de los artículos 13 o 14 del presente Convenio, solamente podrá negarse a atenderla si:

a) La petición es incompatible con las competencias, en materia de protección de datos, de las autoridades habilitadas para responder;

b) la petición no está conforme con lo dispuesto en el presente Convenio;

c) atender a la petición fuese incompatible con la soberanía, la seguridad o el orden público de la Parte que la haya designado, o con los derechos y libertades fundamentales de las personas que estén bajo la jurisdicción de dicha Parte.

Artículo 17. Gastos y procedimientos de asistencia.

1. La ayuda mutua que las Partes se concedan con arreglo a los términos del artículo 13, así como la asistencia qué ellas presten a las personas concernidas residentes en el extranjero con arreglo a los términos del artículo 14, no dará lugar al pago de gastos y derechos que no sean los correspondientes a los expertos y a los intérpretes. Dichos gastos y derechos correrán a cargo de la Parte que haya designado a la autoridad que haya presentado la petición e asistencia.

2. La persona concernida no podrá estar obligada a pagar, en relación con las gestiones emprendidas por su cuenta en el territorio de otra Parte, los gastos y derechos que no sean los exigibles a las personas que residan en el territorio de dicha Parte.

3. Las demás modalidades relativas a la asistencia referentes concretamente a las formas y procedimientos así como a las lenguas que se utilicen se establecerán directamente entre las Partes concernidas.

CAPITULO V.
Comité Consultivo.

Artículo 18. Composición del Comité.

1. Después de la entrada en vigor del presente Convenio se constituirá un Comité Consultivo.

2. Cada Parte designará a un representante y a un suplente en dicho Comité. Cualquier Estado miembro del Consejo de Europa que no sea Parte del Convenio tendrá el derecho de hacerse representar en el Comité por un observador.

3. El Comité Consultivo podrá, mediante una decisión tomada por unanimidad, invitar a cualquier Estado no miembro del Consejo de Europa, que no sea Parte en el Convenio, a hacerse representar por un observador en una de las reuniones.

Artículo 19. Funciones del Comité El Comité Consultivo:

a) Podrá presentar propuestas con el fin de facilitar o de mejorar la aplicación del Convenio;

b) podrá presentar propuestas de enmienda del presente Convenio, con arreglo al artículo 21;

c) formulará su opinión acerca de cualquier propuesta de enmienda al presente Convenio que se le someta, con arreglo al artículo 21, párrafo 3;

d) podrá, a petición de una Parte, expresar su opinión acerca de cualquier cuestión relativa a la aplicación del presente Convenio.

Artículo 20. Procedimiento.

1. El Secretario general del Consejo de Europa convocará al Comité Consultivo. Celebrará su primera reunión en los doce meses que sigan a la entrada en vigor del presente Convenio. Posteriormente se reunirá al menos una vez cada dos años y, en todo caso, cada vez que un tercio de los representantes de las Partes solicite su convocatoria.

2. La mayoría de los representantes de las Partes constituirá el quorum necesario para celebrar una reunión del Comité Consultivo.

3. Después de cada una de dichas reuniones, el Comité Consultivo someterá al Comité de Ministros del Consejo de Europa una memoria acerca de sus trabajos y el funcionamiento del Convenio.

4. Sin perjuicio de lo dispuesto en el presente Convenio, el Comité Consultivo fijará su reglamento anterior.

CAPITULO VI.
Enmiendas.

Artículo 21. Enmiendas.

1. Podrán proponerse enmiendas al presente Convenio por una Parte, por el Comité de Ministros del Consejo de Europa o por el Comité Consultivo.

2. Cualquier propuesta de enmienda se comunicará por el Secretario general del Consejo de Europa ajos Estados miembros del Consejo de Europa y a cada Estado no miembro que se haya adherido o se le haya invitado a que se adhiera al presente Convenio, con arreglo a lo dispuesto en el artículo 23.

3. Además, cualquier modificación propuesta por una Parte o por el Comité de Ministros se comunicará al Comité Consultivo, el cual presentará al Comité de Ministros su opinión acerca de la enmienda propuesta.

4. El Comité de Ministros examinará la enmienda propuesta y cualquier opinión presentada por el Comité Consultivo y podrá aprobar la enmienda.

5. El texto de cualquier enmienda aprobada por el Comité de Ministros conforme al párrafo 4 del presente artículo se remitirá a las Partes para su aceptación.

6. Cualquier enmienda aprobada con arreglo al párrafo 4 del presente artículo entrará en vigor el trigésimo día después de que todas las Partes hayan informado al Secretario general de que la han aceptado.

CAPITULO VII.
Cláusulas finales.

Artículo 22. Entrada en vigor.

1. El presente Convenio quedará abierto a la firma de los Estados miembros del Consejo de Europa. Se someterá a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación se depositarán en poder del Secretario general del Consejo de Europa.

2. El presente Convenio entrará en vigor el día primero del mes siguiente a la expiración de un período de tres meses después de la fecha en que cinco Estados miembros del Consejo de Europa hayan expresado su consentimiento para quedar vinculados por el Convenio, con arreglo a las disposiciones del párrafo anterior.

3. Para cualquier Estado miembro que expresare ulteriormente su consentimiento para quedar vinculado por el Convenio,

éste entrará en vigor el día primero del mes siguiente a la expiración de un período de tres meses después de la fecha del depósito del instrumento de ratificación, aceptación o aprobación.

Artículo 23. Adhesión de Estados no miembros.

1. Después de la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa podrá invitar a cualquier Estado no miembro del Consejo de Europa a que se adhiera el presente Convenio mediante un acuerdo adoptado por la mayoría prevista en el artículo 20, d), del Estatuto del Consejo de Europa y por unanimidad de los representantes de los Estados contratantes que tengan el derecho a formar parte del Comité.

2. Para cualquier Estado adherido, el Convenio entrará en vigor el día primero del mes siguiente a la expiración de un período de tres meses después de la fecha del depósito del instrumento de adhesión en poder del Secretario general del Consejo de Europa.

Artículo 24. Cláusula territorial.

1. Cualquier Estado podrá designar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el territorio o los territorios a los cuales se aplicaré el presente Convenio.

2. Cualquier Estado en cualquier otro momento posterior, y mediante una declaración dirigida al Secretario general del Consejo de Europa, podrá ampliar la aplicación del presente Convenio a cualquier otro territorio designado en la declaración. El Convenio entrará en vigor, con respecto a dicho territorio, el día primero del mes siguiente a la expiración de un período de tres meses después de la fecha de recepción de la declaración por el Secretario general.

3. Cualquier declaración hecha en virtud de los dos párrafos anteriores podrá retirarse, en lo que respecta a cualquier territorio designado en dicha declaración, mediante notificación dirigida al Secretario general La retirada será efectiva el día primero del mes siguiente a la expiración de un período de seis meses después de la fecha de recepción de la notificación por el Secretario general.

Artículo 25. Reservas.

No podrá formularse reserva alguna con respecto a las disposiciones del presente Convenio.

Artículo 26. Denuncia.

1. Cualquier Parte podrá en cualquier momento denunciar el presente Convenio dirigiendo una notificación al Secretario general del Consejo de Europa.

2. La denuncia será efectiva el día primero del mes siguiente a la expiración de un período de seis meses después de la fecha de recepción de la notificación por el Secretario general.

Artículo 27. Notificaciones.

El Secretario general del Consejo de Europa notificará a los Estados miembros del Consejo y a cualquier Estado que se haya adherido al presente Convenio:

a) Cualquier firma;

b) el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;

c) cualquier fecha de entrada en vigor del presente Convenio conforme a sus artículos 22, 23 y 24;

d) cualquier otro acto, notificación o comunicación relativo al presente Convenio.

En fe de lo cual los infrascritos, debidamente autorizados a efecto, firman el presente Convenio.

Hecho en Estrasburgo el 28 de enero de 1981 en francés y en inglés, los dos textos igualmente fehacientes, en un ejemplar único, que quedará depositado en los archivos del Consejo de Europa. El Secretario general del Consejo de Europa remitirá copia certificada conforme del mismo a cada uno de los Estados miembros del Consejo de Europa y a cualquier Estado invitado a la adhesión al presente Convenio.

ESTADOS PARTES		
(1) Alemania, República Federal de	19-6-1985	(R)

España.	31-1-1984	(R)
(2) Francia.:	24-3-1983	(Ap)
(3) Noruega.	20-2-1984	(R)
Suecia.	29-9-1982	(R)
R - Ratificación. Ap - Aprobación.		

DECLARACIONES Y RESERVAS

(1) ALEMANIA, República Federal de.

(Declaraciones contenidas en tres cartas del Representante Permanente de la República Federal de Alemania, fechadas el 19 de junio de 1985.).

Artículo 8, párrafo b) -.

«La República Federal de Alemania parte del principio de que no puede darse ningún curso a una solicitud de informes, de acuerdo con lo que dispone el párrafo b) del artículo 8, si la persona afectada no está en condiciones de justificar suficientemente su petición de información».

Artículo 12, párrafo 2.

«Refiriéndose al apartado 5 del párrafo 67 del Informe explicativo relativo al Convenio para la protección de personas respecto al tratamiento automatizado de datos de carácter personal, el Gobierno de la República Federal de Alemania parte del principio de que el párrafo 2 del artículo 12 deja a las partes la libertad de estimar, en el cuadro de su derecho interno en materia de protección de datos, las normas prohibiendo en ciertos casos particulares la transmisión de datos de carácter personal a fin de tener en cuenta los intereses de la persona afectada dignos de ser protegidos».

Artículo 13, párrafo 2, apartado a).

«La Autoridad competente a nivel de la Federación es:

Der Bundesminister des Innern Postrach 170290 D-5300 Bonn-1.

Las autoridades competentes a nivel de los Estados federados (Lander) serán designadas tan pronto como sean posibles».

Artículo 24, párrafo 1.

«El Convenio se aplica igualmente al Estado federado {Land) de Berlín con efecto de la fecha en la cual entrará en vigor para la República Federal de Alemania».

(2) FRANCIA.

El Gobierno de la República Francesa desea hacer la siguiente declaración:

«Conforme a lo dispuesto en el artículo 3, párrafo 2, apartado c), aplicará el presente Convenio, asimismo, a los ficheros de datos de carácter personal que no sean objeto de tratamientos automatizados».

(3) NORUEGA.

Declaración contenida en el Instrumento de ratificación depositado el 20 de febrero de 1984.

Artículo 3, párrafo 2, apartado a).

«El Convenio se aplicará a ficheros privados de carácter personal que no son utilizados ni en el sector privado ni por sociedades o fundaciones».

Artículo 3, párrafo 2, apartado b).

«Las disposiciones del Convenio se aplicarán igualmente a informaciones referentes a las asociaciones o fundaciones».

Artículo 24, párrafo J.

«El Convenio no se aplicará a Svalbard».

Artículo 13, párrafo 2, apartado a).

«La Autoridad designada en Noruega conforme a lo que dispone el artículo 13, párrafo 2, apartado a), del Convenio es: Datatisynet Postboks 8177 Dep. Oslo 1».

El presente Convenio entró en vigor de forma general y para España el 1 de octubre de 1985, de conformidad con lo establecido en el artículo 22. 2 del mismo.

Lo que se hace público para conocimiento general.

Madrid, 7 de noviembre de 1985.

El secretario general técnico del Ministerio de Justicia del Ministerio de Asuntos Exteriores, José Manuel Paz y Agüeras.

COUNCIL OF EUROPE
COMMITTEE OF MINISTERS

RECOMMENDATION No. R (87) 15

OF THE COMMITTEE OF MINISTERS TO MEMBER STATES

REGULATING THE USE OF PERSONAL DATA IN THE POLICE SECTOR[1]

(Adopted by the Committee of Ministers on 17 September 1987
at the 410th meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Aware of the increasing use of automatically processed personal data in the police sector and of the possible benefits obtained through the use of computers and other technical means in this field;

Taking account also of concern about the possible threat to the privacy of the individual arising through the misuse of automated processing methods;

Recognising the need to balance the interests of society in the prevention and suppression of criminal offences and the maintenance of public order on the one hand and the interests of the individual and his right to privacy on the other;

Bearing in mind the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and in particular the derogations permitted under Article 9;

Aware also of the provisions of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms,

Recommends the governments of member states to:

— be guided in their domestic law and practice by the principles appended to this recommendation, and

— ensure publicity for the provisions appended to this recommendation and in particular for the rights which its application confers on individuals.

---

1. When this recommendation was adopted:

— in accordance with Article 10.2.*c* of the Rules of Procedure for the meetings of the Ministers' Deputies, the Representative of Ireland reserved the right of his Government to comply with it or not, the Representative of the United Kingdom reserved the right of her Government to comply or not with Principles 2.2 and 2.4 of the recommendation, and the Representative of the Federal Republic of Germany reserved the right of his Government to comply or not with Principle 2.1 of the recommendation;

— in accordance with Article 10.2.*d* of the said Rules of Procedure, the Representative of Switzerland abstained, stating that he reserved the right of his Government to comply with it or not and underlining that his abstention should not be interpreted as expressing disapproval of the recommendation as a whole.

Appendix to Recommendation No. R (87) 15

Scope and definitions

The principles contained in this recommendation apply to the collection, storage, use and communication of personal data for police purposes which are the subject of automatic processing.

For the purposes of this recommendation, the expression "personal data" covers any information relating to an identified or identifiable individual. An individual shall not be regarded as "identifiable" if identification requires an unreasonable amount of time, cost and manpower.

The expression "for police purposes" covers all the tasks which the police authorities must perform for the prevention and suppression of criminal offences and the maintenance of public order.

The expression "responsible body" (controller of the file) denotes the authority, service or any other public body which is competent according to national law to decide on the purpose of an automated file, the categories of personal data which must be stored and the operations which are to be applied to them.

A member state may extend the principles contained in this recommendation to personal data not undergoing automatic processing.

Manual processing of data should not take place if the aim is to avoid the provisions of this recommendation.

A member state may extend the principles contained in this recommendation to data relating to groups of persons, associations, foundations, companies, corporations or any other body consisting directly or indirectly of individuals, whether or not such bodies possess legal personality.

The provisions of this recommendation should not be interpreted as limiting or otherwise affecting the possibility for a member state to extend, where appropriate, certain of these principles to the collection, storage and use of personal data for purposes of state security.

Basic principles

Principle 1 — Control and notification

1.1. Each member state should have an independent supervisory authority outside the police sector which should be responsible for ensuring respect for the principles contained in this recommendation.

1.2. New technical means for data processing may only be introduced if all reasonable measures have been taken to ensure that their use complies with the spirit of existing data protection legislation.

1.3. The responsible body should consult the supervisory authority in advance in any case where the introduction of automatic processing methods raises questions about the application of this recommendation.

1.4. Permanent automated files should be notified to the supervisory authority. The notification should specify the nature of each file declared, the body responsible for its processing, its purposes, the type of data contained in the file and the persons to whom the data are communicated.

Ad hoc files which have been set up at the time of particular inquiries should also be notified to the supervisory authority either in accordance with the conditions settled with the latter, taking account of the specific nature of these files, or in accordance with national legislation.

Principle 2 — Collection of data

2.1. The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation.

2.2. Where data concerning an individual have been collected and stored without his knowledge, and unless the data are deleted, he should be informed, where practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced.

2.3. The collection of data by technical surveillance or other automated means should be provided for in specific provisions.

2.4. The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry.

Principle 3 — Storage of data

3.1. As far as possible, the storage of personal data for police purposes should be limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks within the framework of national law and their obligations arising from international law.

3.2. As far as possible, the different categories of data stored should be distinguished in accordance with their degree of accuracy or reliability and, in particular, data based on facts should be distinguished from data based on opinions or personal assessments.

3.3. Where data which have been collected for administrative purposes are to be stored permanently, they should be stored in a separate file. In any case, measures should be taken so that administrative data are not subject to rules applicable to police data.

Principle 4 — Use of data by the police

4. Subject to Principle 5, personal data collected and stored by the police for police purposes should be used exclusively for those purposes.

Principle 5 — Communication of data

5.1. *Communication within the police sector*

The communication of data between police bodies to be used for police purposes should only be permissible if there exists a legitimate interest for such communication within the framework of the legal powers of these bodies.

5.2.i. *Communication to other public bodies*

Communication of data to other public bodies should only be permissible if, in a particular case:

a. there exists a clear legal obligation or authorisation, or with the authorisation of the supervisory authority, or if

b. these data are indispensable to the recipient to enable him to fulfil his own lawful task and provided that the aim of the collection or processing to be carried out by the recipient is not incompatible with the original processing, and the legal obligations of the communicating body are not contrary to this.

5.2.ii. Furthermore, communication to other public bodies is exceptionally permissible if, in a particular case:

a. the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if

b. the communication is necessary so as to prevent a serious and imminent danger.

5.3.i. *Communication to private parties*

The communication of data to private parties should only be permissible if, in a particular case, there exists a clear legal obligation or authorisation, or with the authorisation of the supervisory authority.

5.3.ii. Communication to private parties is exceptionally permissible if, in a particular case:

a. the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if

b. the communication is necessary so as to prevent a serious and imminent danger.

5.4. *International communication*

Communication of data to foreign authorities should be restricted to police bodies. It should only be permissible:

a. if there exists a clear legal provision under national or international law,

b. in the absence of such a provision, if the communication is necessary for the prevention of a serious and imminent danger or is necessary for the suppression of a serious criminal offence under ordinary law,

and provided that domestic regulations for the protection of the person are not prejudiced.

5.5.i. *Requests for communication*

Subject to specific provisions contained in national legislation or in international agreements, requests for communication of data should provide indications as to the body or person requesting them as well as the reason for the request and its objective.

5.5.ii. *Conditions for communication*

As far as possible, the quality of data should be verified at the latest at the time of their communication. As far as possible, in all communications of data, judicial decisions, as well as decisions not to prosecute, should be indicated and data based on opinions or personal assessments checked at source before being communicated and their degree of accuracy or reliability indicated.

If it is discovered that the data are no longer accurate and up to date, they should not be communicated. If data which are no longer accurate or up to date have been communicated, the communicating body should inform as far as possible all the recipients of the data of their non-conformity.

5.5.iii. *Safeguards for communication*

The data communicated to other public bodies, private parties and foreign authorities should not be used for purposes other than those specified in the request for communication.

Use of the data for other purposes should, without prejudice to paragraphs 5.2 to 5.4 of this principle, be made subject to the agreement of the communicating body.

5.6. *Interconnection of files and on-line access to files*

The interconnection of files with files held for different purposes is subject to either of the following conditions :

a. the grant of an authorisation by the supervisory body for the purposes of an inquiry into a particular offence, or

b. in compliance with a clear legal provision.

Direct access/on-line access to a file should only be allowed if it is in accordance with domestic legislation which should take account of Principles 3 to 6 of this recommendation.

Principle 6 — Publicity, right of access to police files, right of rectification and right of appeal

6.1. The supervisory authority should take measures so as to satisfy itself that the public is informed of the existence of files which are the subject of notification as well as of its rights in regard to these files. Implementation of this principle should take account of the specific nature of *ad hoc* files, in particular the need to avoid serious prejudice to the performance of a legal task of the police bodies.

6.2. The data subject should be able to obtain access to a police file at reasonable intervals and without excessive delay in accordance with the arrangements provided for by domestic law.

6.3. The data subject should be able to obtain, where appropriate, rectification of his data which are contained in a file.

Personal data which the exercise of the right of access reveals to be inaccurate or which are found to be excessive, inaccurate or irrelevant in application of any of the other principles contained in this recommendation should be erased or corrected or else be the subject of a corrective statement added to the file.

Such erasure or corrective measures should extend as far as possible to all documents accompanying the police file and, if not done immediately, should be carried out, at the latest, at the time of subsequent processing of the data or of their next communication.

6.4. Exercise of the rights of access, rectification and erasure should only be restricted insofar as a restriction is indispensable for the performance of a legal task of the police or is necessary for the protection of the data subject or the rights and freedoms of others.

In the interests of the data subject, a written statement can be excluded by law for specific cases.

6.5. A refusal or a restriction of those rights should be reasoned in writing. It should only be possible to refuse to communicate the reasons insofar as this is indispensable for the performance of a legal task of the police or is necessary for the protection of the rights and freedoms of others.

6.6. Where access is refused, the data subject should be able to appeal to the supervisory authority or to another independent body which shall satisfy itself that the refusal is well founded.

Principle 7 — Length of storage and updating of data

7.1. Measures should be taken so that personal data kept for police purposes are deleted if they are no longer necessary for the purposes for which they were stored.

For this purpose, consideration shall in particular be given to the following criteria : the need to retain data in the light of the conclusion of an inquiry into a particular case ; a final judicial decision, in particular an acquittal ; rehabilitation ; spent convictions ; amnesties ; the age of the data subject, particular categories of data.

7.2. Rules aimed at fixing storage periods for the different categories of personal data as well as regular checks on their quality should be established in agreement with the supervisory authority or in accordance with domestic law.

Principle 8 — Data security

8. The responsible body should take all the necessary measures to ensure the appropriate physical and logical security of the data and prevent unauthorised access, communication or alteration.

The different characteristics and contents of files should, for this purpose, be taken into account.

interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.

3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.

4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

Artículo 19. *Derecho a indemnización.*

1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.

3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

TÍTULO IV

Disposiciones sectoriales

CAPÍTULO I

Ficheros de titularidad pública

Artículo 20. *Creación, modificación o supresión.*

1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:

a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

3. En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Artículo 21. *Comunicación de datos entre Administraciones públicas.*

1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.

3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.

4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

Artículo 22. *Ficheros de las Fuerzas y Cuerpos de Seguridad.*

1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23. *Excepciones a los derechos de acceso, rectificación y cancelación.*

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del

artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Artículo 24. *Otras excepciones a los derechos de los afectados.*

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.

2. Lo dispuesto en el artículo 15 y en el apartado 1 del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.

CAPÍTULO II

Ficheros de titularidad privada

Artículo 25. *Creación.*

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26. *Notificación e inscripción registral.*

1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.

En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

Artículo 27. *Comunicación de la cesión de datos.*

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.

Artículo 28. *Datos incluidos en las fuentes de acceso público.*

1. Los datos personales que figuren en el censo promocional, o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3, j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.

2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial.

Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes.

La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.

3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique.

En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.

4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica.

Artículo 29. *Prestación de servicios de información sobre solvencia patrimonial y crédito.*

1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos

III

(Actos adoptados en aplicación del Tratado UE)

ACTOS ADOPTADOS EN APLICACIÓN DEL TÍTULO VI DEL TRATADO UE

DECISIÓN MARCO 2008/977/JAI DEL CONSEJO

de 27 de noviembre de 2008

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

EL CONSEJO DE LA UNIÓN EUROPEA,

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

Vista la propuesta de la Comisión,

Visto el dictamen del Parlamento Europeo [1],

Considerando lo siguiente:

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

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

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

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

(5) El intercambio de datos personales en el marco de la cooperación policial y judicial en materia penal, especialmente con arreglo al principio de disponibilidad de la información establecido en el Programa de La Haya, debe basarse en normas claras que aumenten la confianza mutua entre las autoridades competentes y garanticen la protección de la correspondiente información excluyendo toda discriminación respecto de esta cooperación entre los Estados miembros y garantizando al mismo tiempo el pleno respeto de los derechos fundamentales de la persona. Los instrumentos existentes a escala europea no bastan; la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [3], no se aplica al tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las contempladas en el título VI del Tratado de la Unión Europea, ni, en ningún caso, a las operaciones de tratamiento de datos relacionadas con la seguridad pública, la defensa, la seguridad del Estado o las actuaciones del Estado en materia penal.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

HA ADOPTADO LA PRESENTE DECISIÓN MARCO:

Artículo 1

Objetivo y ámbito de aplicación

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

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

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

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

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

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

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

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

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

Artículo 2

Definiciones

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

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

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

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

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

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

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

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

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

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

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

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

Artículo 3

Principios de licitud, proporcionalidad y finalidad

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

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

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

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

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

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

Artículo 4

Rectificación, supresión y bloqueo

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

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

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

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

Artículo 5

Fijación de plazos de supresión y comprobación

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

Artículo 6

Tratamiento de categorías especiales de datos

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

Artículo 7

Decisiones específicas automatizadas

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

Artículo 8

Control de calidad de los datos transmitidos o disponibles

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

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

Artículo 9

Plazos

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

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

Artículo 10

Registro y documentación

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

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

Artículo 11

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

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

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

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

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

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

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

Artículo 12

Cumplimiento de las limitaciones nacionales de tratamiento

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

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

Artículo 13

Transferencia a autoridades competentes de terceros Estados y a organismos internacionales

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

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

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

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

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

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

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

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

   i) legítimos intereses específicos del interesado, o

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

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

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

Artículo 14

Transmisión a particulares en los Estados miembros

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

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

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

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

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

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

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

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

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

Artículo 15

Información a petición de las autoridades competentes

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

Artículo 16

Información al interesado

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

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

Artículo 17

Derecho de acceso a los datos

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

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

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

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

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

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

c) para proteger la seguridad pública;

d) para proteger la seguridad del Estado;

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

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

Artículo 18

Derecho de rectificación, supresión o bloqueo

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

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

Artículo 19

Derecho a reparación

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

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

Artículo 20

Vías de recurso

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

Artículo 21

Confidencialidad del tratamiento

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

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

Artículo 22

Seguridad del tratamiento

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artículo 23

Consulta previa

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

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

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

Artículo 24

Sanciones

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

Artículo 25

Autoridades nacionales de control

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

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

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

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

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

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

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

Artículo 26

Relación con acuerdos con terceros Estados

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

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

Artículo 27

Evaluación

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

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

Artículo 28

Relación con actos de la Unión adoptados previamente

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

Artículo 29

Aplicación

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

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

Artículo 30

Entrada en vigor

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

Hecho en Bruselas, el 27 de noviembre de 2008.

Por el Consejo

La Presidenta

M. ALLIOT-MARIE