

**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 lista 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 datos.

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 cuales 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 seguridad 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 capítulo.

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 hacia 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 datos;

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 hacer 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 que 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 a los 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 aplicará 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 Postfach 170290 D-5300 Bonn-1.

Las autoridades competentes a nivel de los Estados federados (Länder) 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 SECTOR¹

*(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.

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.

I. Disposiciones generales

JEFATURA DEL ESTADO

23750 LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

JUAN CARLOS I
REY DE ESPAÑA

A todos los que la presente vieren y entendieren.
Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica.

TÍTULO I

Disposiciones generales

Artículo 1. Objeto.

La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Artículo 2. Ámbito de aplicación.

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable

del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

a) Los ficheros regulados por la legislación de régimen electoral.

b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.

d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.

e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Artículo 3. Definiciones.

A los efectos de la presente Ley Orgánica se entenderá por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.

j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

TÍTULO II

Principios de la protección de datos

Artículo 4. *Calidad de los datos.*

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificadas o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 5. *Derecho de información en la recogida de datos.*

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Artículo 6. *Consentimiento del afectado.*

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Artículo 7. *Datos especialmente protegidos.*

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 8. *Datos relativos a la salud.*

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de

carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Artículo 9. *Seguridad de los datos.*

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. *Deber de secreto.*

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11. *Comunicación de datos.*

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

- a) Cuando la cesión está autorizada en una ley.
- b) Cuando se trate de datos recogidos de fuentes accesibles al público.
- c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
- d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
- e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
- f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 12. *Acceso a los datos por cuenta de terceros.*

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

TÍTULO III

Derechos de las personas

Artículo 13. *Impugnación de valoraciones.*

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 14. *Derecho de consulta al Registro General de Protección de Datos.*

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Artículo 15. *Derecho de acceso.*

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

Artículo 16. *Derecho de rectificación y cancelación.*

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán rectificadas o canceladas, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

4. Si los datos rectificadas o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Artículo 17. *Procedimiento de oposición, acceso, rectificación o cancelación.*

1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.

2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

Artículo 18. *Tutela de los derechos.*

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los

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 tendientes 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 registrarán 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

de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.

3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.

Artículo 30. *Tratamientos con fines de publicidad y de prospección comercial.*

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.

4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Artículo 31. *Censo promocional.*

1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.

2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público.

3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos

procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado.

4. Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.

Artículo 32. *Códigos tipo.*

1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.

2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

TÍTULO V

Movimiento internacional de datos

Artículo 33. *Norma general.*

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. *Excepciones.*

Lo dispuesto en el artículo anterior no será de aplicación:

- a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
- b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
- c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.
- d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
- e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
- f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
- g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
- h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
- i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquella sea acorde con la finalidad del mismo.
- k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

TÍTULO VI

Agencia de Protección de Datos

Artículo 35. *Naturaleza y régimen jurídico.*

1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.

2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.

3. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.

4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

- a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.
- b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.
- c) Cualesquiera otros que legalmente puedan serle atribuidos.

5. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 36. *El Director.*

1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.

2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas.

En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.

3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1, a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.

4. El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales.

Artículo 37. *Funciones.*

Son funciones de la Agencia de Protección de Datos:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.

d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.

e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.

n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

Artículo 38. *Consejo Consultivo.*

El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

Un Diputado, propuesto por el Congreso de los Diputados.

Un Senador, propuesto por el Senado.

Un representante de la Administración Central, designado por el Gobierno.

Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.

Un miembro de la Real Academia de la Historia, propuesto por la misma.

Un experto en la materia, propuesto por el Consejo Superior de Universidades.

Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.

Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.

Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.

El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 39. *El Registro General de Protección de Datos.*

1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos:

a) Los ficheros de que sean titulares las Administraciones públicas.

b) Los ficheros de titularidad privada.

c) Las autorizaciones a que se refiere la presente Ley.

d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.

e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Artículo 40. *Potestad de inspección.*

1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.

A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 41. *Órganos correspondientes de las Comunidades Autónomas.*

1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido.

2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.

3. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Artículo 42. *Ficheros de las Comunidades Autónomas en materia de su exclusiva competencia.*

1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas

correctoras que determine en el plazo que expresamente se fije en el requerimiento.

2. Si la Administración pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

TÍTULO VII

Infracciones y sanciones

Artículo 43. *Responsables.*

1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.

2. Cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 46, apartado 2.

Artículo 44. *Tipos de infracciones.*

1. Las infracciones se calificarán como leves, graves o muy graves.

2. Son infracciones leves:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.

e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

3. Son infracciones graves:

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.

b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

4. Son infracciones muy graves:

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Artículo 45. *Tipo de sanciones.*

1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.

2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas.

3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas.

4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.

6. En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.

7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 46. *Infracciones de las Administraciones públicas.*

1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las Administraciones públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas.

3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Artículo 47. *Prescripción.*

1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.

6. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 48. *Procedimiento sancionador.*

1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título.

2. Las resoluciones de la Agencia de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.

Artículo 49. *Potestad de inmovilización de ficheros.*

En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

Disposición adicional primera. *Ficheros preexistentes.*

Los ficheros y tratamientos automatizados inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.

En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica, y la obligación prevista en el párrafo anterior deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

Disposición adicional segunda. *Ficheros y Registro de Población de las Administraciones públicas.*

1. La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población.

2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada Administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones públicas.

Disposición adicional tercera. *Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social.*

Los expedientes específicamente instruidos al amparo de las derogadas Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social, que contengan datos de cualquier índole susceptibles de afectar a la seguridad, al honor, a la intimidad o a la imagen de las personas, no podrán ser consultados sin que medie consentimiento expreso de los afectados, o hayan transcurrido cincuenta años desde la fecha de aquéllos.

En este último supuesto, la Administración General del Estado, salvo que haya constancia expresa del fallecimiento de los afectados, pondrá a disposición del solicitante la documentación, suprimiendo de la misma los datos aludidos en el párrafo anterior, mediante la utilización de los procedimientos técnicos pertinentes en cada caso.

Disposición adicional cuarta. *Modificación del artículo 112.4 de la Ley General Tributaria.*

El apartado cuarto del artículo 112 de la Ley General Tributaria pasa a tener la siguiente redacción:

«4. La cesión de aquellos datos de carácter personal, objeto de tratamiento, que se debe efectuar a la Administración tributaria conforme a lo dispuesto en el artículo 111, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito tampoco será de aplicación lo que respecto a las Administraciones públicas establece el apartado 1 del artículo 21 de la Ley Orgánica de Protección de Datos de carácter personal.»

Disposición adicional quinta. *Competencias del Defensor del Pueblo y órganos autonómicos semejantes.*

Lo dispuesto en la presente Ley Orgánica se entiende sin perjuicio de las competencias del Defensor del Pueblo y de los órganos análogos de las Comunidades Autónomas.

Disposición adicional sexta. *Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados.*

Se modifica el artículo 24.3, párrafo 2.º de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados, con la siguiente redacción:

«Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la ley.

También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable

del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.

En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado.»

Disposición transitoria primera. *Tratamientos creados por Convenios internacionales.*

La Agencia de Protección de Datos será el organismo competente para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal respecto de los tratamientos establecidos en cualquier Convenio Internacional del que sea parte España que atribuya a una autoridad nacional de control esta competencia, mientras no se cree una autoridad diferente para este cometido en desarrollo del Convenio.

Disposición transitoria segunda. *Utilización del censo promocional.*

Reglamentariamente se desarrollarán los procedimientos de formación del censo promocional, de oposición a aparecer en el mismo, de puesta a disposición de sus solicitantes, y de control de las listas difundidas. El Reglamento establecerá los plazos para la puesta en operación del censo promocional.

Disposición transitoria tercera. *Subsistencia de normas preexistentes.*

Hasta tanto se lleven a efectos las previsiones de la disposición final primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo; 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley.

Disposición derogatoria única. *Derogación normativa.*

Queda derogada la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal.

Disposición final primera. *Habilitación para el desarrollo reglamentario.*

El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley.

Disposición final segunda. *Preceptos con carácter de Ley ordinaria.*

Los Títulos IV, VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la disposición adicional cuarta, la disposición transitoria primera y la final primera tienen el carácter de Ley ordinaria.

Disposición final tercera. *Entrada en vigor.*

La presente Ley entrará en vigor en el plazo de un mes, contado desde su publicación en el «Boletín Oficial del Estado».

Por tanto,

Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta Ley Orgánica.

Madrid, 13 de diciembre de 1999.

JUAN CARLOS R.

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 persona-

les 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 la 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 Estado 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) n° 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 otros 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 afectar 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 dimensiones 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, garantías 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 com-

petentes, 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 garantizan 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

(Actos adoptados en aplicación del título VI del Tratado de la Unión Europea)

DECISIÓN MARCO 2006/960/JAI DEL CONSEJO

de 18 de diciembre de 2006

sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de la Unión Europea, y en particular su artículo 30, apartado 1, letras a) y b), y su artículo 34, apartado 2, letra b),

Vista la iniciativa del Reino de Suecia,

Visto el dictamen del Parlamento Europeo,

Considerando lo siguiente:

- (1) Uno de los principales objetivos de la Unión Europea es ofrecer a los ciudadanos un alto grado de seguridad dentro de un espacio de libertad, seguridad y justicia.
- (2) Este objetivo habrá de lograrse previendo y combatiendo la delincuencia mediante una mayor cooperación entre los servicios de seguridad de los Estados miembros, respetando al mismo tiempo los principios y las normas sobre derechos humanos, libertades fundamentales y el Estado de Derecho, principios en los que se basa la Unión Europea y que son comunes a los Estados miembros.
- (3) El intercambio de información e inteligencia sobre la delincuencia y las actividades delictivas es la base de la cooperación policial en la Unión para alcanzar el objetivo general de aumentar la seguridad de sus ciudadanos.
- (4) El oportuno acceso a información e inteligencia que sean fiables y actualizadas es fundamental para que los servicios de seguridad puedan descubrir, prevenir e investigar con éxito delitos y actividades delictivas, en particular en un espacio en el que se han suprimido los controles en las fronteras interiores. Puesto que las actividades delictivas se cometen de forma clandestina, es necesario controlarlas e intercambiar con especial rapidez la información al respecto.
- (5) Es importante que la posibilidad de que los servicios de seguridad obtengan de los demás Estados miembros información e inteligencia sobre los delitos graves y los actos de terrorismo se plantee de manera horizontal, y no en función de las diferencias entre formas de delincuencia, ni en función del reparto de competencias entre autoridades policiales y judiciales.
- (6) Actualmente, los procedimientos formales, las estructuras administrativas y los obstáculos jurídicos establecidos en la legislación de los Estados miembros están limitando gravemente el intercambio rápido y eficaz de información e inteligencia entre los servicios de seguridad. Esta situación es inaceptable para los ciudadanos de la Unión Europea, y, por consiguiente, se pide mayor seguridad y una actuación policial más eficiente, al mismo tiempo que se protegen los derechos humanos.
- (7) Es necesario que los servicios de seguridad puedan solicitar y obtener información e inteligencia de otros Estados miembros en las distintas fases de la investigación, desde la fase de recogida de inteligencia criminal hasta la fase de investigación criminal. Los sistemas de los Estados miembros difieren a este respecto, pero la presente Decisión marco no pretende modificarlos. Sin embargo, sí se propone garantizar, con respecto a algunos tipos de información e inteligencia, que dentro de la Unión determinada información de vital importancia para los servicios de seguridad se intercambie con rapidez.
- (8) La inexistencia de un marco jurídico común para el intercambio rápido y eficaz de información e inteligencia entre los servicios de seguridad de los Estados miembros es una carencia que debe subsanarse, por lo que el Consejo de la Unión Europea considera necesario adoptar un instrumento jurídicamente vinculante sobre la simplificación del intercambio de información e inteligencia. La presente Decisión marco no debe afectar a aquellos instrumentos ya existentes o futuros que permitan ampliar o facilitar los procedimientos de intercambio de información e inteligencia, como el Convenio de 18 de diciembre de 1997 celebrado sobre la base del artículo K.3 del Tratado de la Unión Europea, relativo a la asistencia mutua y la cooperación entre las Administraciones aduaneras ⁽¹⁾.
- (9) En lo que se refiere al intercambio de información, la presente Decisión marco se entiende sin perjuicio de los intereses esenciales en materia de seguridad nacional, del desarrollo de una investigación en curso o de la seguridad de personas o actividades de inteligencia específicas en el ámbito de la seguridad del Estado.

⁽¹⁾ DO C 24 de 23.1.1998, p. 2.

- (10) Es importante promover un intercambio de información todo lo amplio posible, especialmente en lo referente a los delitos directa o indirectamente vinculados a la delincuencia organizada y al terrorismo, y de manera que no haga disminuir el necesario nivel de cooperación entre los Estados miembros según los acuerdos existentes.
- (11) Al perseguir el interés común de los Estados miembros de luchar contra la delincuencia transfronteriza debe hallarse un equilibrio adecuado entre la rapidez y eficacia de la cooperación policial y los principios y normas acordados en materia de protección de datos, libertades fundamentales, derechos humanos y libertades individuales.
- (12) En la Declaración sobre la lucha contra el terrorismo, adoptada por el Consejo Europeo en su sesión del 25 de marzo de 2004, el Consejo Europeo encargó al Consejo que estudiara medidas para la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros.
- (13) Por lo que respecta a Islandia y Noruega, la presente Decisión marco constituye un desarrollo de las disposiciones del acervo de Schengen que pertenecen al ámbito del artículo 1 de la Decisión 1999/437/CE del Consejo, de 17 de mayo de 1999, relativa a determinadas normas de desarrollo 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 ⁽¹⁾. En la presente Decisión marco se han seguido los procedimientos establecidos en dicho Acuerdo.
- (14) Por lo que respecta a Suiza, la presente Decisión marco constituye un desarrollo de las disposiciones del acervo de Schengen, en los términos del Acuerdo firmado entre la Unión Europea, la Comunidad Europea y la Confederación Suiza en relación con la asociación de la Confederación Suiza a la ejecución, aplicación y desarrollo del acervo de Schengen, que entra en el ámbito contemplado en el artículo 1(H) de la Decisión 1999/437/CE interpretado conjuntamente con el apartado 1 del artículo 4 de la Decisión 2004/860/CE del Consejo, de 25 de octubre de 2004, relativa a la firma, en nombre de la Comunidad Europea y a la aplicación provisional de determinadas disposiciones de dicho Acuerdo ⁽²⁾, y con el apartado 1 del artículo 4 de la Decisión 2004/849/CE del Consejo, de 25 de octubre de 2004, relativa a la firma, en nombre de la Unión Europea, y a la aplicación provisional de determinadas disposiciones de dicho Acuerdo ⁽³⁾.

⁽¹⁾ DO L 176 de 10.7.1999, p. 31.

⁽²⁾ DO L 370 de 17.12.2004, p. 78.

⁽³⁾ DO L 368 de 15.12.2004, p. 26.

HA ADOPTADO LA PRESENTE DECISIÓN MARCO:

TÍTULO I

ÁMBITO DE APLICACIÓN Y DEFINICIONES

Artículo 1

Objetivo y ámbito de aplicación

1. El objetivo de la presente Decisión marco es establecer las normas en virtud de las cuales los servicios de seguridad de los Estados miembros puedan intercambiar de forma rápida y eficaz la información e inteligencia disponibles para llevar a cabo investigaciones criminales u operaciones de inteligencia criminal.

2. La presente Decisión marco se entenderá sin perjuicio de los acuerdos bilaterales o multilaterales entre los Estados miembros y terceros países y de los instrumentos de la Unión Europea sobre asistencia jurídica mutua y reconocimiento mutuo de las resoluciones en materia penal, incluida cualquier condición establecida por terceros países relativa al uso de la información una vez facilitada.

3. La presente Decisión marco se refiere a toda la información e inteligencia, tal como se define en la letra d) del artículo 2. No impone a los Estados miembros obligación alguna de recoger y almacenar información e inteligencia con el objetivo de facilitarla a los servicios de seguridad competentes de otro Estado Miembro.

4. La presente Decisión marco no impone a los Estados miembros obligación alguna de facilitar información e inteligencia para que se utilice como prueba ante una autoridad judicial, ni confiere derecho alguno a utilizar dicha información o inteligencia con ese fin. Cuando un Estado miembro haya obtenido información o inteligencia de conformidad con la presente Decisión marco y desee utilizarla como prueba ante una autoridad judicial, deberá obtener el consentimiento del Estado miembro que haya facilitado la información o inteligencia empleando, cuando resulte necesario en virtud de la legislación nacional del Estado miembro que haya facilitado la información o inteligencia, los instrumentos vigentes sobre cooperación judicial entre los Estados miembros. No será necesario recabar dicho consentimiento si el Estado miembro requerido ya hubiera accedido, en el momento de la transmisión de la inteligencia o información, a que ésta se utilizara como prueba.

5. La presente Decisión marco no impone al Estado miembro que recibe la solicitud de información o inteligencia obligación alguna de obtenerla mediante medidas coercitivas, definidas de conformidad con la legislación nacional.

6. Cuando lo permita su legislación nacional, y de conformidad con ella, los Estados miembros facilitarán información o inteligencia obtenida con anterioridad a la solicitud mediante medidas coercitivas.

7. La presente Decisión marco no supondrá modificación de la obligación de respetar los derechos fundamentales y los principios jurídicos básicos plasmados en el artículo 6 del Tratado de la Unión Europea, ni se verá afectada ninguna obligación que incumba a los servicios de seguridad a este respecto.

Artículo 2

Definiciones

A efectos de la presente Decisión marco se entenderá por:

- a) servicio de seguridad competente: la autoridad nacional policial, aduanera u otra, autorizada según el Derecho interno a descubrir, prevenir e investigar delitos y actividades delictivas y a ejercer la autoridad y adoptar medidas coercitivas en el contexto de esas actividades. Las agencias o unidades que traten especialmente cuestiones de seguridad nacional no quedan cubiertas por el concepto de «servicio de seguridad competente». A más tardar el 18 de diciembre de 2007, cada Estado miembro indicará mediante una declaración, que quedará depositada en la Secretaría General del Consejo, qué autoridades están comprendidas en el concepto de «servicio de seguridad competente». Esta declaración podrá modificarse en cualquier momento.
- b) investigación criminal: fase del procedimiento dentro de la cual los servicios de seguridad o las autoridades judiciales competentes, incluido el Ministerio fiscal, adoptan medidas para el establecimiento y averiguación de los hechos, los sospechosos y las circunstancias en relación con uno o varios actos delictivos concretos comprobados.
- c) operación de inteligencia criminal: fase del procedimiento que no ha alcanzado aún la fase de investigación criminal, dentro de la cual el Derecho interno autoriza a un servicio de seguridad competente a recoger, tratar y analizar información sobre delitos o actividades delictivas para establecer si se han cometido actos delictivos concretos o se pueden cometer en el futuro.
- d) información y/o inteligencia:
 - i) todo tipo de información o datos en poder de los servicios de seguridad;

- ii) todo tipo información o datos en poder de autoridades públicas o entes privados, de la que puedan disponer los servicios de seguridad sin tener que utilizar medidas coercitivas de conformidad con el artículo 1, apartado 5.

- e) delitos enumerados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI, de 13 de junio de 2002, relativa a la orden de detención europea ⁽¹⁾ (denominados en lo sucesivo «delitos enumerados en el artículo 2, apartado 2, de la Decisión marco 2002/584/JAI»): los delitos contemplados en la legislación nacional que corresponden o equivalen a los enumerados en dicha disposición.

TÍTULO II

INTERCAMBIO DE INFORMACIÓN E INTELIGENCIA

Artículo 3

Suministro de información e inteligencia

1. Los Estados miembros garantizarán que la información e inteligencia puedan facilitarse a los servicios de seguridad competentes de otros Estados miembros con arreglo a la presente Decisión marco.
2. Se facilitará información e inteligencia a petición de los servicios de seguridad competentes que, actuando de conformidad con los poderes que le haya conferido el Derecho interno, lleven a cabo una investigación criminal o una operación de inteligencia criminal.
3. Los Estados miembros garantizarán que el suministro de información e inteligencia a los servicios de seguridad competentes de otros Estados miembros no esté supeditado a condiciones más estrictas que las aplicables a escala nacional para el suministro y la solicitud de información e inteligencia. En particular, los Estados miembros no supeditarán a la obtención de una aprobación o autorización judicial el suministro, por parte del servicio de seguridad nacional competente a un servicio de seguridad competente de otro Estado miembro, de información o inteligencia a la que el servicio de seguridad competente requerido habría podido acceder sin aprobación o autorización judicial si se tratara de un procedimiento interno.
4. Cuando, con arreglo al Derecho nacional del Estado miembro requerido, el servicio de seguridad competente requerido sólo pueda acceder a la información o inteligencia solicitada al amparo de una aprobación o autorización de una autoridad judicial, el servicio de seguridad competente requerido tendrá la obligación de solicitar a la autoridad judicial competente una aprobación o autorización de acceso y de intercambio de la información solicitada. En su resolución, la autoridad judicial competente del Estado miembro requerido aplicará los mismos criterios, sin perjuicio del artículo 10, apartados 1 y 2, que si se tratara de un asunto exclusivamente interno.

5. Cuando la información o inteligencia solicitada se haya obtenido de otro Estado miembro o de un tercer país y esté sujeta a la regla de la especialidad, su transmisión al servicio de seguridad competente de otro Estado miembro únicamente podrá realizarse con el consentimiento del Estado miembro o del tercer país que proporcionó dicha información o inteligencia.

Artículo 4

Plazos para el suministro de información e inteligencia

1. Los Estados miembros se dotarán de procedimientos que les permitan responder en el plazo máximo de ocho horas a las solicitudes urgentes de información e inteligencia relativas a delitos enumerados en el artículo 2, apartado 2, de la Decisión marco 2002/584/JAI, cuando la información o inteligencia solicitada se encuentre en una base de datos a la que tenga acceso directo un servicio de seguridad.

2. En caso de que el servicio de seguridad competente requerido no pueda responder en el plazo de ocho horas, comunicará los motivos por medio del formulario cuyo modelo se recoge en el anexo A. Si el suministro de la información o inteligencia solicitadas dentro del plazo de ocho horas supone una carga desproporcionada para el servicio de seguridad competente requerido, éste podrá aplazar dicho suministro. En tal caso, deberá informar inmediatamente al servicio de seguridad competente requerido de tal aplazamiento y proporcionarle la información o inteligencia solicitadas lo antes posible y, a más tardar, en un plazo de tres días. La aplicación de las disposiciones en virtud del presente apartado se revisará a más tardar el 19 de diciembre de 2009.

3. Los Estados miembros deberán asegurarse de que se responda en un plazo de una semana a las solicitudes no urgentes de información e inteligencia relativas a los delitos enumerados en el artículo 2, apartado 2, de la Decisión marco 2002/584/JAI, siempre que la información o inteligencia solicitada se encuentre en una base de datos a la que un servicio de seguridad competente requerido no pueda responder en el plazo de una semana, comunicará los motivos por medio del formulario cuyo modelo se recoge en el anexo A.

4. En todos los demás casos, los Estados miembros velarán por que la información solicitada se comunique al servicio de seguridad competente requerido en el plazo de 14 días. En caso de que el servicio de seguridad competente requerido no pueda responder en el plazo de 14 días, comunicará los motivos por medio del formulario cuyo modelo se recoge en el anexo A.

Artículo 5

Solicitudes de información e inteligencia

1. Se podrá solicitar información e inteligencia a efectos de descubrimiento, prevención o investigación de un delito cuando existan razones de hecho para creer que otro Estado miembro dispone de información e inteligencia pertinente. La petición deberá exponer dichas razones de hecho y explicar para qué fin se solicita la información o inteligencia y la vinculación existente entre ese fin y la persona objeto de la información o inteligencia.

2. El servicio de seguridad competente requirente se abstendrá de solicitar más información o inteligencia de la necesaria para el fin que persigue la solicitud y de establecer plazos más cortos de los necesarios para dicho fin.

3. Las solicitudes de información o inteligencia contendrán al menos la información indicada en el anexo B.

Artículo 6

Cauces y lengua de comunicación

1. El intercambio de información e inteligencia en virtud de la presente Decisión marco se llevará a cabo a través de cualquiera de los cauces de cooperación policial internacional existentes. La lengua utilizada para la solicitud y el intercambio de información será la aplicable para el cauce utilizado. Al realizar las declaraciones a que se refiere el artículo 2, letra a), los Estados miembros facilitarán asimismo a la Secretaría General del Consejo los datos de los puntos de contacto a los que pueden enviarse solicitudes en caso de urgencia. Estos datos podrán modificarse en cualquier momento. La Secretaría General del Consejo comunicará las declaraciones recibidas a los Estados miembros y a la Comisión.

2. La información o inteligencia se intercambiará también con Europol de conformidad con el Convenio basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (Convenio Europol) ⁽¹⁾ y con Eurojust de conformidad con la Decisión 2002/187/JAI del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia ⁽²⁾, en la medida en que el intercambio se refiera a un delito o una actividad delictiva que entre en sus respectivas competencias.

⁽¹⁾ DO C 316 de 27.11.1995, p. 2. Convenio cuya última modificación la constituye el Protocolo establecido sobre la base del artículo 43, apartado 1, del Convenio Europol (DO C 2 de 6.1.2004, p. 3).

⁽²⁾ DO L 63 de 6.3.2002, p. 1. Decisión cuya última modificación la constituye la Decisión 2003/659/JAI (DO L 245 de 29.9.2003, p. 44).

*Artículo 7***Intercambio espontáneo de información e inteligencia**

1. No obstante lo dispuesto en el artículo 10, y sin necesidad de solicitud previa, los servicios de seguridad competentes de un Estado miembro facilitarán a los servicios de seguridad competentes de los demás Estados miembros interesados información e inteligencia cuando haya razones de hecho para creer que esa información e inteligencia pueden ayudar al descubrimiento, la prevención o la investigación de delitos enumerados en el artículo 2, apartado 2, de la Decisión marco 2002/584/JAI. Las modalidades de este intercambio espontáneo se regirán por la legislación nacional de los Estados miembros que faciliten la información.

2. El suministro de información e inteligencia se limitará a lo que se considere pertinente y necesario para el descubrimiento, prevención o investigación satisfactorios del delito o actividad delictiva de que se trate.

*Artículo 8***Protección de datos**

1. Los Estados miembros velarán por que las reglas sobre protección de datos establecidas a efectos de la utilización de los canales de comunicación a que se refiere el artículo 6, apartado 1, se apliquen también al procedimiento de intercambio de información e inteligencia previsto en la presente Decisión marco.

2. La utilización de la información e inteligencia que hayan sido intercambiadas de manera directa o bilateral con arreglo a la presente Decisión marco estará sujeta a las disposiciones nacionales sobre protección de datos del Estado miembro receptor, en el cual dichas información e inteligencia estarán sujetas a las mismas normas de protección que si hubieran sido recabadas en el propio Estado miembro. Los datos personales que sean objeto de tratamiento en el contexto de la aplicación de la presente Decisión marco estarán protegidos de conformidad con el Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y, para los Estados miembros que lo hayan ratificado, su Protocolo adicional, de 8 de noviembre de 2001, relativo a las autoridades de control y los tránsitos transfronterizos de datos. También deberán tenerse en cuenta los principios de la Recomendación R (87) 15 del Consejo de Europa, dirigida a regular la utilización de datos de carácter personal en el sector de la policía, cuando los servicios de seguridad manejen datos personales obtenidos en virtud de la presente Decisión marco.

3. Los servicios de seguridad competentes del Estado miembro al que se hayan proporcionado información e inteligencia en virtud de la presente Decisión marco sólo podrán utilizarlas para los fines para los cuales fueron facilitadas, de conformidad con lo dispuesto en la presente Decisión marco, o para prevenir una amenaza grave e inminente a la seguridad pública; el tratamiento de dicha información para otros fines sólo se permitirá con la autorización previa del Estado miembro transmisor y estará sujeto a la legislación nacional del Estado miembro receptor. La autorización podrá concederse siempre y cuando así lo permita la legislación del Estado miembro transmisor.

4. El servicio de seguridad competente que facilite información e inteligencia de conformidad con la presente Decisión marco podrá, con arreglo a su Derecho interno, imponer condiciones para el uso de la información e inteligencia al servicio de seguridad competente destinatario. También podrá imponer condiciones relativas a la notificación de los resultados de la investigación criminal o de la operación de inteligencia criminal en cuyo contexto se haya producido el intercambio de información e inteligencia. El servicio de seguridad competente receptor estará obligado a respetar dichas condiciones salvo en aquellos casos en que el Derecho nacional establezca excepciones a esas limitaciones en beneficio de las autoridades judiciales, de los órganos legislativos o de cualquier otro órgano independiente creado en virtud de la ley y encargado de la supervisión de los servicios de seguridad competentes. En dichos casos, sólo se podrá utilizar la información e inteligencia previa consulta al Estado miembro transmisor, cuyos intereses y opiniones se tendrán en cuenta en la medida de lo posible. En casos específicos, el Estado miembro transmisor podrá pedir al Estado miembro receptor explicaciones sobre el uso y posterior tratamiento de la información e inteligencia transmitida.

*Artículo 9***Confidencialidad**

Los servicios de seguridad competentes tendrán debidamente en cuenta, en cada uno de los intercambios de información o inteligencia, las obligaciones en materia de secreto de la investigación. Para ello, los servicios de seguridad competentes garantizarán, de conformidad con su Derecho interno, la confidencialidad de toda la información e inteligencia de carácter confidencial que se haya facilitado.

*Artículo 10***Motivos para no comunicar información o inteligencia**

1. Sin perjuicio de lo dispuesto en el artículo 3, apartado 3, los servicios de seguridad competentes sólo podrán negarse a facilitar información o inteligencia cuando razones de hecho hagan suponer que el suministro de la información o inteligencia:

a) perjudicaría intereses esenciales en materia de seguridad nacional del Estado miembro requerido,

o

b) comprometería el éxito de una investigación en curso o de una operación de inteligencia criminal o la seguridad de las personas,

o

c) sería claramente desproporcionado o irrelevante para el fin que persigue la solicitud.

2. Cuando la solicitud se refiera a un delito castigado con pena de prisión igual o inferior a un año con arreglo a la legislación del Estado miembro requerido, el servicio de seguridad competente podrá negarse a facilitar la información o inteligencia requerida.

3. El servicio de seguridad competente se negará a facilitar la información o inteligencia solicitadas si la autoridad judicial competente no ha autorizado el acceso y el intercambio de la información solicitada con arreglo al artículo 3, apartado 4.

TÍTULO III

DISPOSICIONES FINALES

Artículo 11

Ejecución

1. Los Estados miembros tomarán las medidas necesarias para dar cumplimiento a lo dispuesto en la presente Decisión marco antes del 19 de diciembre de 2006

2. Los Estados miembros transmitirán a la Secretaría General del Consejo y a la Comisión el texto de las disposiciones que incorporen a su Derecho interno las obligaciones derivadas de la presente Decisión marco. Sobre la base de esa y otras informaciones facilitadas, previa solicitud, por los Estados miembros, la Comisión presentará al Consejo, antes del 19 de diciembre de 2006, un informe sobre la aplicación de la presente Decisión marco. A más tardar el 19 de diciembre de 2006, el Consejo verificará en qué medida los Estados miembros han dado cumplimiento a lo dispuesto en la presente Decisión marco.

Artículo 12

Relación con otros instrumentos

1. Las disposiciones del artículo 39, apartados 1, 2 y 3, y del artículo 46 del Convenio de Aplicación del Acuerdo de Schengen ⁽¹⁾, en la medida en que se refieren al intercambio de información e inteligencia a efectos de la realización de investigaciones criminales y de operaciones de inteligencia criminal previstas en la presente Decisión marco, se sustituirán por las disposiciones de la presente Decisión marco.

2. Quedan derogadas la Decisión del Comité ejecutivo de Schengen de 16 de diciembre de 1998 relativa a la cooperación policial transfronteriza en el ámbito de la prevención e investigación de hechos delictivos (SCH/Com-ex (98) 51 rev 3) ⁽²⁾ y la Decisión del Comité ejecutivo de Schengen de 28 de abril de 1999 relativa a la cooperación policial para la prevención e investigación de hechos delictivos (SCH/Com-ex (99) 18) ⁽³⁾.

3. Los Estados miembros podrán continuar aplicando los acuerdos bilaterales o multilaterales en vigor cuando se adopte la presente Decisión marco, siempre que tales acuerdos permitan ampliar los objetivos de la presente Decisión marco y ayuden a simplificar o facilitar en mayor grado los procedimientos de intercambio de información e inteligencia contenidos en el ámbito de aplicación de la presente Decisión marco.

4. Los Estados miembros podrán celebrar o poner en vigor acuerdos bilaterales o multilaterales una vez que la presente Decisión marco haya entrado en vigor, siempre que tales acuerdos permitan ampliar los objetivos de la presente Decisión marco y ayuden a simplificar o facilitar en mayor grado los procedimientos de intercambio de información e inteligencia contenidos en el ámbito de aplicación de la presente Decisión marco.

5. Los acuerdos a que se refieren los apartados 3 y 4 no podrán afectar en ningún caso a las relaciones con los Estados miembros que no sean parte en ellos.

⁽¹⁾ DO L 239 de 22.9.2000, p. 19. Convenio cuya última modificación la constituye el Reglamento (CE) n.º 1160/2005 del Parlamento Europeo y del Consejo (DO L 191 de 22.7.2005, p. 18).

⁽²⁾ DO L 239 de 22.9.2000, p. 407.

⁽³⁾ DO L 239 de 22.9.2000, p. 421.

6. A más tardar el 19 de diciembre de 2006, los Estados miembros notificarán al Consejo y a la Comisión los acuerdos en vigor mencionados en el apartado 3 que desean seguir aplicando.

7. Los Estados miembros notificarán también al Consejo y a la Comisión cualquier nuevo acuerdo mencionado en el apartado 4, en los tres meses siguientes a su firma o, en lo que respecta a los instrumentos que ya hayan sido firmados antes de la adopción de la presente Decisión marco, a su entrada en vigor.

Artículo 13

Entrada en vigor

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

Hecho en 18 de diciembre de 2006

Por el Consejo

El Presidente

J.-E. ENESTAM

ANEXO A

INTERCAMBIO DE INFORMACIÓN EN VIRTUD DE LA DECISIÓN MARCO 2006/960/JAI DEL CONSEJO
FORMULARIO QUE UTILIZARÁ EL ESTADO MIEMBRO REQUERIDO EN CASO DE
TRANSMISIÓN/RETRASO/DENEGACIÓN DE INFORMACIÓN

El presente formulario se utilizará para transmitir la información y/o inteligencia requerida, para informar a la autoridad requirente de la imposibilidad de cumplir el plazo normal, de la necesidad de presentar la solicitud a la autorización de una autoridad judicial, o bien de la denegación de transmisión de la información.

El presente formulario podrá utilizarse más de una vez durante el procedimiento (p. ej., si la solicitud debe presentarse primero a una autoridad judicial y luego se pone de manifiesto que la ejecución de la solicitud debe denegarse).

Autoridad requerida (nombre, dirección, teléfono, fax, correo electrónico, Estado miembro):	
Datos del funcionario responsable (facultativo):	
Número de referencia de la presente respuesta:	
Fecha y número de referencia de la respuesta anterior:	
Respondiendo a la siguiente autoridad requirente:	
Fecha y hora de la solicitud:	
Número de referencia de la solicitud:	
Plazo normal con arreglo al artículo 4 de la Decisión marco 2006/960/JAI	
El delito está recogido en el artículo 2, apartado 2, de la Decisión marco 2002/584/JAI y La información o inteligencia solicitada se conserva en una base de datos a la que tiene acceso directo un servicio de seguridad en el Estado miembro requerido	La solicitud es urgente → <input type="checkbox"/> 8 horas
	La solicitud no es urgente → <input type="checkbox"/> 1 semana
Demás casos	→ <input type="checkbox"/> 14 días

Información transmitida de acuerdo con la Decisión marco 2006/960/JAI : Información e inteligencia facilitada	
1. La utilización de la información o de la inteligencia facilitada	
<input type="checkbox"/>	Únicamente se autorizará para los fines para los que se haya facilitado o para prevenir una amenaza grave e inminente a la seguridad pública;
<input type="checkbox"/>	Se autorizará asimismo a otros efectos, sin perjuicio de las siguientes condiciones (facultativo):
2. Fiabilidad de la fuente	
<input type="checkbox"/>	Fiable
<input type="checkbox"/>	Fiable en general
<input type="checkbox"/>	No fiable
<input type="checkbox"/>	No puede evaluarse
3. Exactitud de la información o inteligencia	
<input type="checkbox"/>	Segura
<input type="checkbox"/>	Certificada por la fuente
<input type="checkbox"/>	Rumores confirmados
<input type="checkbox"/>	Rumores no confirmados

<p>4. Los resultados de la investigación criminal o de la operación de inteligencia criminal que haya originado el intercambio de información e inteligencia deben comunicarse a la autoridad transmisora</p> <p><input type="checkbox"/> Sí <input type="checkbox"/> No</p>
<p>5. En caso de intercambio espontáneo: motivos que permitan creer que la información o inteligencia podrían contribuir a la detección, prevención o investigación de los delitos enumerados en el artículo 2, apartado 2, de la Decisión marco 2002/584/JAI:</p>

<p>RETRASO – No es posible responder en el plazo aplicable previsto en el artículo 4 de la Decisión marco 2006/960/JAI</p>
<p>No es posible facilitar la información o inteligencia en el plazo indicado por los siguientes motivos:</p>
<p>Es probable que se pueda facilitar dentro de:</p> <p><input type="checkbox"/> 1 día <input type="checkbox"/> 2 días <input type="checkbox"/> 3 días <input type="checkbox"/> ... semanas <input type="checkbox"/> 1 mes</p>
<p><input type="checkbox"/> Se ha solicitado la autorización de una autoridad judicial. Se espera que el procedimiento que lleva a la concesión/denegación de la autorización dure ... semanas</p>

<p>DENEGACIÓN – La información o inteligencia <input type="checkbox"/> no ha podido facilitarse y solicitarse en el plano nacional, o <input type="checkbox"/> no puede facilitarse por uno o varios de los siguientes motivos:</p>
<p>A – Motivo relacionado con un control judicial que impide la transmisión o requiere recurrir a la asistencia jurídica mutua</p>
<p><input type="checkbox"/> la autoridad judicial competente no ha autorizado el acceso y el intercambio de información o inteligencia</p>
<p><input type="checkbox"/> la información o inteligencia solicitada se obtuvo previamente mediante medidas coercitivas y la legislación nacional no permite su comunicación</p>
<p><input type="checkbox"/> la información o inteligencia no está en posesión</p> <ul style="list-style-type: none"> ▪ de un servicio de seguridad; o ▪ de autoridades públicas o entidades privadas de un modo que permita a un servicio de seguridad disponer de ella sin la adopción de medidas coercitivas
<p><input type="checkbox"/> B – La comunicación de la información o inteligencia solicitada perjudicaría intereses esenciales de seguridad nacional o comprometería el éxito de una investigación en curso o de una operación de inteligencia criminal o la seguridad de personas, o resultaría claramente desproporcionada o irrelevante respecto de los fines para los que se ha solicitado.</p>
<p>En caso de utilizar la casilla A o B, indique, si lo considera necesario, información adicional o los motivos (...) de denegación (facultativo):</p>
<p><input type="checkbox"/> D – La autoridad requerida ha decidido denegar la ejecución debido a que la solicitud se refiere, en la legislación del Estado miembro requerido, al siguiente delito (especifique la naturaleza del delito y su tipificación jurídica) castigado con pena de prisión igual o inferior a un año.</p>
<p><input type="checkbox"/> E – La información o inteligencia solicitada no está disponible.</p>
<p><input type="checkbox"/> F – La información o inteligencia solicitada se ha obtenido de otro Estado miembro o de un tercer país y está sometida a la regla de la especialidad, y dicho Estado miembro o tercer país no ha dado su consentimiento para la transmisión de la información o inteligencia.</p>

ANEXO B

INTERCAMBIO DE INFORMACIÓN EN VIRTUD DE LA DECISIÓN MARCO 2006/960/JAI DEL CONSEJO
 FORMULARIO DE SOLICITUD DE INFORMACIÓN E INTELIGENCIA QUE UTILIZARÁ
 EL ESTADO MIEMBRO REQUIRENTE

El presente formulario se utilizará cuando se solicite información e inteligencia en virtud de la Decisión marco 2006/960/JAI

I – Información administrativa

Autoridad requirente (nombre, dirección, teléfono, fax, correo electrónico, Estado miembro):	
Datos del funcionario responsable (facultativo):	
Al Estado miembro siguiente:	
Fecha y hora de la presente solicitud:	
Número de referencia de la presente solicitud:	

Solicitudes anteriores				
<input type="checkbox"/> Es la primera solicitud sobre este asunto				
<input type="checkbox"/> Se han presentado anteriormente las siguientes solicitudes para este mismo asunto				
Solicitud(es) anterior(es)			Respuesta(s)	
	Fecha	Número de referencia (en el Estado miembro requirente)	Fecha	Número de referencia (en el Estado miembro requerido)
1.				
2.				
3.				
4.				

Si la solicitud se remite a más de una autoridad del Estado miembro requerido, indicar todos los canales utilizados:	
<input type="checkbox"/> Funcionario de enlace en Europol/UNE	<input type="checkbox"/> Para información <input type="checkbox"/> Para ejecución
<input type="checkbox"/> Interpol/OCN	<input type="checkbox"/> Para información <input type="checkbox"/> Para ejecución
<input type="checkbox"/> Sirene	<input type="checkbox"/> Para información <input type="checkbox"/> Para ejecución
<input type="checkbox"/> Funcionario de enlace	<input type="checkbox"/> Para información <input type="checkbox"/> Para ejecución
<input type="checkbox"/> Otros (especificar):	<input type="checkbox"/> Para información <input type="checkbox"/> Para ejecución
Si la misma solicitud se remite a otro Estado miembro, indicar de qué Estados miembros se trata y los canales utilizados (facultativo)	

II – Plazos

Recordatorio: plazos con arreglo al artículo 4 de la Decisión marco 2006/960/JAI

A – El delito está recogido en el artículo 2, apartado 2, de la Decisión marco 2002/584/JAI

y

La información o inteligencia solicitada se conserva en una base de datos a la que tiene acceso directo un servicio de seguridad

→ La solicitud es urgente → Plazo: 8 horas con posibilidad de aplazamiento

→ La solicitud no es urgente → Plazo: 1 semana

B – Demás casos: plazo: 14 días

Se solicita tratar con urgencia

NO se solicita tratar con urgencia

Motivos de la urgencia (p. ej.: sospechosos detenidos, el asunto debe presentarse ante un tribunal antes de una fecha concreta)

Información o inteligencia solicitada

Tipos De Delito O Actividad Delictiva Investigados

Descripción de las circunstancias de la comisión del delito o delitos, incluido el momento, lugar y grado de participación en ellos de la persona objeto de la información o inteligencia solicitada:

Naturaleza del delito o delitos

A – Aplicación de los apartados 1 o 3 del artículo 4 de la Decisión marco 2006/960/JAI

A.1. El delito está penado con una pena máxima privativa de libertad de al menos tres años en el Estado miembro requirente Y

A.2. El delito es uno (o varios) de los siguientes:

- | | |
|--|--|
| <input type="checkbox"/> pertenencia a organización delictiva | <input type="checkbox"/> blanqueo del producto del delito |
| <input type="checkbox"/> terrorismo | <input type="checkbox"/> falsificación de moneda, con inclusión del euro |
| <input type="checkbox"/> trata de seres humanos | <input type="checkbox"/> delito informático |
| <input type="checkbox"/> explotación sexual de menores y pornografía infantil | <input type="checkbox"/> delitos contra el medio ambiente, incluido el tráfico ilícito de especies animales protegidas y de especies y variedades vegetales protegidas |
| <input type="checkbox"/> tráfico ilícito de estupefacientes y sustancias psicotrópicas | <input type="checkbox"/> ayuda a la entrada y a la estancia irregulares |
| <input type="checkbox"/> tráfico ilícito de armas, municiones y explosivos | <input type="checkbox"/> homicidio, lesiones graves |
| <input type="checkbox"/> corrupción | <input type="checkbox"/> tráfico ilícito de órganos y tejidos humanos |
| <input type="checkbox"/> fraude, incluido el que afecte a los intereses financieros de las Comunidades Europeas con arreglo al Convenio de 26 de julio de 1995 relativo a la protección de los intereses financieros de las Comunidades Europeas | <input type="checkbox"/> secuestro, detención ilegal y toma de rehenes |
| <input type="checkbox"/> atraco organizado o a mano armada | <input type="checkbox"/> racismo y xenofobia |
| <input type="checkbox"/> tráfico ilícito de bienes culturales, incluidas las antigüedades y las obras de arte | <input type="checkbox"/> tráfico ilícito de materiales radiactivos o sustancias nucleares |
| <input type="checkbox"/> estafa | <input type="checkbox"/> tráfico de vehículos robados |
| <input type="checkbox"/> chantaje y extorsión | <input type="checkbox"/> violación |
| <input type="checkbox"/> falsificación y piratería de productos | <input type="checkbox"/> incendio provocado |
| <input type="checkbox"/> falsificación de documentos administrativos y tráfico de documentos falsos | <input type="checkbox"/> delitos incluidos en el ámbito de competencia de la Corte Penal Internacional |
| <input type="checkbox"/> falsificación de medios de pago | <input type="checkbox"/> secuestro de aeronaves y buques |
| <input type="checkbox"/> tráfico ilícito de sustancias hormonales y otros factores de crecimiento | <input type="checkbox"/> sabotaje |

→ Por consiguiente, el delito está recogido en el artículo 2, apartado 2, de la Decisión marco 2002/584/JAI. Por tanto, el artículo 4, apartado 1 (casos urgentes) y el artículo 4, apartado 3 (casos no urgentes) de la Decisión marco .../.../ JAI se aplican en relación con los plazos que se han de cumplir para responder a la presente solicitud.

- B – El delito o delitos no están recogidos en la letra A.
- En tal caso, descripción del delito o delitos:

Fin para el que se solicita la información o inteligencia**Vinculación entre el fin para el cual se solicita la información o inteligencia y la persona objeto de la información o inteligencia****Identidad o identidades (en la medida en que se conozcan) de la persona o personas objeto principal de la investigación criminal o de la operación de inteligencia criminal en las que se fundamenta la solicitud de la información o inteligencia****Motivos que inducen a pensar que la información o inteligencia se encuentran en el Estado miembro requerido****Restricciones a la utilización de la información que figura en la solicitud con fines distintos de aquellos para los que se facilitó o para prevenir una amenaza inminente y grave para la seguridad pública**

- utilización autorizada
 utilización autorizada, a condición de que no se mencione su procedencia
 utilización no autorizada salvo autorización de quien la transmite
 utilización no autorizada

I. DISPOSICIONES GENERALES

JEFATURA DEL ESTADO

12134 *Ley 31/2010, de 27 de julio, sobre simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea.*

JUAN CARLOS I,

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.
Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley:

PREÁMBULO

Uno de los principales objetivos de la Unión Europea es ofrecer a los ciudadanos un alto grado de seguridad dentro de un espacio de libertad, seguridad y justicia.

Este objetivo habrá de lograrse previendo y combatiendo la delincuencia mediante una mayor cooperación entre los servicios de seguridad de los Estados miembros de la Unión Europea (en adelante Estados miembros), respetando al mismo tiempo los principios y las normas sobre derechos humanos, libertades fundamentales y el Estado de Derecho, principios en los que se basa la Unión Europea y que son comunes a los Estados miembros.

En la Declaración sobre la lucha contra el terrorismo, adoptada por el Consejo Europeo en su sesión del 25 de marzo de 2004, el Consejo Europeo encargó al Consejo que estudiara medidas para la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros.

A tal fin, el Consejo ha adoptado la Decisión Marco 2006/960/JAI, de 18 de diciembre, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea, que constituye un instrumento jurídicamente vinculante sobre la simplificación del intercambio de información e inteligencia.

El intercambio de información e inteligencia sobre la delincuencia y las actividades delictivas es la base de la cooperación policial y aduanera en la Unión Europea para alcanzar el objetivo general de aumentar la seguridad de sus ciudadanos.

El acceso a la información e inteligencia fiables y actualizadas es fundamental para que los servicios de seguridad puedan descubrir, prevenir e investigar con éxito delitos y actividades delictivas, en particular en un espacio en el que se han suprimido los controles en las fronteras interiores. Puesto que las actividades delictivas se cometen de forma clandestina, es necesario controlarlas e intercambiar con especial rapidez la información al respecto.

Por ello, es necesario que los servicios de seguridad españoles puedan intercambiar información e inteligencia de otros Estados miembros en las distintas fases de la investigación, desde la fase de recogida de inteligencia criminal hasta la fase de investigación criminal. La presente Ley se propone garantizar, con respecto a algunos tipos de información e inteligencia, que determinada información de vital importancia para los servicios de seguridad españoles y de los países de los Estados miembros se intercambie con rapidez. Es precisamente ese intercambio de información sobre datos personales en muchos casos lo que justifica que el texto haya sido informado por la Agencia Española de Protección de Datos en sentido favorable.

En lo que se refiere al intercambio de información, esta Ley se entiende sin perjuicio de los intereses esenciales en materia de seguridad nacional, del desarrollo de una investigación en curso o de la seguridad de personas o actividades de inteligencia específicas en el ámbito de la seguridad del Estado.

Los Estados miembros persiguen, en el ámbito de la seguridad común, luchar contra la delincuencia transfronteriza. En consecuencia, debe hallarse un equilibrio adecuado entre la rapidez y eficacia de la cooperación policial y aduanera, y entre los principios y normas acordados en materia de protección de datos, libertades fundamentales, derechos humanos y libertades individuales, respetando los contenidos jurisprudenciales de las sentencias que en estas materias se adopten por los Tribunales nacionales o internacionales.

En consecuencia de todo lo anteriormente expuesto, mediante esta Ley se incorpora a nuestro ordenamiento jurídico la Decisión Marco del Consejo 2006/960/JAI, de 18 de diciembre, regulando el intercambio de información e inteligencia entre los servicios de seguridad españoles, y los respectivos servicios de seguridad de los demás Estados miembros.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto y ámbito de aplicación.*

1. Esta Ley tiene por objeto establecer las normas en virtud de las cuales un servicio de seguridad español competente podrá intercambiar con los servicios de seguridad competentes de los Estados miembros de la Unión Europea (en adelante Estados miembros) la información e inteligencia disponibles para llevar a cabo:

a) Operaciones de inteligencia criminal consistentes en la recogida, tratamiento y análisis de información por los servicios de seguridad competentes sobre delitos o actividades delictivas con carácter previo a la investigación criminal para establecer si se han cometido actos delictivos concretos o se pueden cometer en el futuro.

b) Investigaciones criminales por los servicios de seguridad o las autoridades judiciales competentes encaminadas a adoptar las medidas necesarias para el establecimiento y descubrimiento de los hechos, los sospechosos y las circunstancias en relación con uno o varios actos delictivos concretos comprobados.

2. La presente Ley se entenderá sin perjuicio de los Acuerdos Bilaterales o Multilaterales entre el Reino de España y los Estados miembros y terceros países y de los instrumentos de la Unión Europea sobre asistencia jurídica mutua y reconocimiento mutuo de las resoluciones en materia penal, incluida cualquier condición establecida por terceros países relativa al uso de la información una vez facilitada.

3. Esta Ley no será de aplicación al intercambio de información e inteligencia que lleve a cabo el Centro Nacional de Inteligencia en el ámbito de los Acuerdos Internacionales ratificados por el Reino de España en materia de protección mutua de la información clasificada y en el ámbito de las relaciones de cooperación y colaboración con servicios de inteligencia de otros países o de Organismos Internacionales para el mejor cumplimiento de sus objetivos.

Artículo 2. *Información e inteligencia.*

A los efectos de lo previsto en la presente Ley se entenderá por información e inteligencia:

- a) Todo tipo de información o datos en poder de los servicios de seguridad.
- b) Todo tipo de información o datos en poder de autoridades públicas o entes privados, de la que puedan disponer los servicios de seguridad sin tener que utilizar medidas coercitivas definidas de acuerdo con la legislación española.

Artículo 3. *Servicios de seguridad competentes.*

A los efectos de lo previsto en esta Ley tendrán la consideración de servicios de seguridad competentes las autoridades policiales y aduaneras, que estén autorizadas por el ordenamiento jurídico español para descubrir, prevenir e investigar delitos y actividades delictivas, así como para ejercer la autoridad y adoptar medidas coercitivas que sean designadas de acuerdo con lo dispuesto en la disposición adicional primera de la Ley, sin perjuicio de lo previsto en el apartado tercero del artículo 1 de esta Ley.

Artículo 4. *Cauces y lengua de comunicación.*

1. El intercambio de información e inteligencia en virtud de la presente Ley se llevará a cabo a través de cualquiera de los canales normalizados de cooperación policial y aduanera internacionales existentes. La lengua utilizada para la solicitud y el intercambio de información será la aplicable para el canal de comunicación empleado.

2. La información o inteligencia se intercambiará también con Europol de conformidad con el Convenio basado en el artículo K.3 del Tratado de la Unión Europea por el que se crea una Oficina Europea de Policía (Convenio Europol) y con Eurojust, de conformidad con la Decisión del Consejo 2002/187/JAI, de 28 de febrero, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia, y la Ley 16/2006, de 26 de mayo, por la que se regula el Estatuto del Miembro Nacional de Eurojust y las relaciones con este órgano de la Unión Europea, en la medida en que el intercambio se refiera a un delito o una actividad delictiva que entre en sus respectivas competencias.

Artículo 5. *Confidencialidad.*

Los servicios de seguridad españoles tendrán en cuenta, en cada uno de los intercambios de información o inteligencia, las obligaciones en materia de secreto de la investigación. Para ello, dichos servicios garantizarán, de conformidad con el ordenamiento jurídico nacional, la confidencialidad de toda la información e inteligencia que se haya facilitado.

Artículo 6. *Protección de datos.*

1. Los canales de comunicación a que se refiere el apartado primero del artículo 4 de esta Ley, así como el procedimiento de intercambio de información e inteligencia previsto en la presente Ley se realizarán de acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en particular con lo dispuesto en su artículo 37.

2. La utilización de la información e inteligencia por los servicios de seguridad españoles que haya sido intercambiada de manera directa o bilateral con arreglo a esta Ley estará sujeta a las disposiciones nacionales sobre protección de datos. Dicha información e inteligencia se regirán por las mismas normas de protección que si hubieran sido recabadas en España.

3. A los efectos de lo establecido en el apartado 2.a) del artículo 11 de la Ley Orgánica 15/1999, de 13 de diciembre, se autoriza la cesión de datos de carácter personal a los servicios de seguridad competentes de los Estados miembros en los términos establecidos en la presente Ley.

4. La cesión de datos obtenidos por la Administración Tributaria en el desempeño de sus funciones se regirá por su normativa específica.

5. Los datos personales, que sean objeto de tratamiento en el contexto de la aplicación de esta Ley, están protegidos de conformidad con el Convenio del Consejo de Europa de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y, para los Estados miembros que lo hayan ratificado, su Protocolo Adicional, de 8 de noviembre de 2001, relativo a las autoridades de control y los tránsitos transfronterizos de datos. Asimismo, deberán tenerse en cuenta los principios de la Recomendación R (87) 15 del Consejo de Europa,

dirigida a regular la utilización de datos de carácter personal en el sector de la policía, cuando los servicios de seguridad manejen datos personales obtenidos en virtud de la presente Ley.

CAPÍTULO II

Solicitud de información e inteligencia por los servicios españoles de seguridad competentes a los servicios de seguridad competentes de otros Estados miembros

Artículo 7. Solicitudes de información e inteligencia.

1. Los servicios de seguridad españoles competentes designados de acuerdo con lo dispuesto en la disposición adicional primera de esta Ley podrán solicitar información e inteligencia a los servicios de seguridad de otro Estado Miembro, al efecto de descubrir, prevenir e investigar la comisión de un delito cuando existan fundadas razones de hecho para creer que el Estado al que se dirige la solicitud dispone de la información e inteligencia pertinente, para lo cual se utilizarán cualquiera de los cauces de cooperación policial o aduanera internacional existentes.

2. La solicitud de información e inteligencia se ajustará al formulario que apruebe el Ministro del Interior y en ella se deberán exponer las razones de hecho a las que se refiere el apartado anterior, el fin para el que se solicita la información o inteligencia, y la vinculación existente entre ese fin y la persona afectada por la solicitud.

3. El servicio de seguridad español competente se abstendrá de solicitar más información o inteligencia de la necesaria para el fin que se persigue y de establecer plazos más cortos de los necesarios para dicho fin.

4. Esta Ley no impone a los Estados miembros obligación alguna de facilitar información e inteligencia para que se utilice como prueba ante una autoridad judicial española, ni confiere derecho alguno a utilizar dicha información e inteligencia con ese fin. Cuando se haya obtenido información o inteligencia de conformidad con la presente Ley y se quiera utilizarla como prueba ante una Autoridad judicial española, deberá obtenerse el consentimiento del Estado miembro que haya facilitado la información o inteligencia empleando, cuando resulte necesario en virtud de la legislación nacional del Estado miembro que haya facilitado la información, los instrumentos vigentes sobre cooperación judicial entre los Estados miembros. No será necesario recabar dicho consentimiento si el Estado miembro requerido ya hubiera accedido en el momento de la transmisión de la inteligencia o información a que ésta se utilizara como prueba.

5. Cuando por los servicios de seguridad españoles competentes pueda deducirse que la información o inteligencia solicitada haya de resultar relevante a efectos de prueba en un procedimiento ante una Autoridad judicial española, en el momento de la solicitud se procederá a recabar el consentimiento del Estado miembro para su utilización a tal fin.

Artículo 8. Tratamiento de la información e inteligencia.

1. El servicio de seguridad español competente al que se le haya proporcionado información e inteligencia en virtud de esta Ley, sólo podrá utilizarla para los fines que fue facilitada, de conformidad con lo dispuesto en la presente Ley, o para prevenir una amenaza grave e inminente a la seguridad pública.

2. El tratamiento de dicha información para otros fines sólo se permitirá con la autorización previa del Estado transmisor cuando así lo permita su legislación, y quedará sujeto a lo dispuesto en el ordenamiento jurídico español.

3. El servicio español de seguridad competente estará obligado a respetar las condiciones establecidas por el servicio de seguridad transmisor de la información, de conformidad con lo previsto en su legislación nacional, salvo en aquellos casos en que el Derecho nacional establezca excepciones a esas limitaciones en beneficio de las Autoridades judiciales, de los órganos legislativos o de cualquier órgano independiente creado en virtud de la Ley y encargado de la supervisión de los servicios de seguridad

competentes. En dichos casos, sólo se podrá utilizar la información e inteligencia previa consulta al Estado miembro transmisor, cuyos intereses y opiniones se tendrán en cuenta en la medida de lo posible. En casos específicos, el Estado miembro transmisor podrá pedir al Estado español explicaciones sobre el uso y posterior tratamiento de la información e inteligencia transmitida.

CAPÍTULO III

Suministro de información e inteligencia por los servicios españoles de seguridad competentes a otros Estados miembros

Artículo 9. Suministro de información e inteligencia.

1. Se facilitará información e inteligencia a petición de los servicios de seguridad competentes de otros Estados miembros que, actuando de conformidad con los poderes que le haya conferido su ordenamiento jurídico nacional, lleven a cabo una investigación criminal o una operación de inteligencia criminal.

2. El suministro de información e inteligencia se llevará a cabo en cada caso por el servicio de seguridad competente que tenga en su poder la información solicitada.

3. Se garantizará que el suministro de información e inteligencia a los servicios de seguridad competentes de otros Estados miembros no esté supeditado a condiciones más estrictas que las aplicables a escala nacional para el suministro y la solicitud de información e inteligencia. En particular, no se supeditará el suministro de información o inteligencia a la obtención de una autorización judicial si el servicio de seguridad español competente hubiera podido acceder a la misma sin autorización judicial de haberse tratado de un procedimiento interno.

4. Cuando con arreglo a lo dispuesto en nuestro ordenamiento jurídico, sólo resulte posible el acceso a la información solicitada al amparo de una autorización judicial, el servicio de seguridad español competente deberá solicitar autorización judicial previa al órgano jurisdiccional competente, para el acceso y suministro de la información solicitada. En su resolución, el órgano jurisdiccional aplicará los mismos criterios que si se tratara de un asunto exclusivamente interno, sin perjuicio de lo dispuesto en los apartados primero y segundo del artículo 11.

5. Cuando la información o inteligencia solicitada se haya obtenido de otro Estado miembro o de un tercer país, su transmisión al servicio de seguridad competente de otro Estado miembro únicamente podrá realizarse con el consentimiento del Estado miembro o del tercer país que proporcionó dicha información o inteligencia.

6. Cuando se reciba una petición urgente de información e inteligencia proveniente de un servicio de seguridad competente de otro Estado miembro, el punto o puntos de contacto nacionales designados de acuerdo con lo previsto en el apartado segundo de la disposición adicional primera de la presente Ley la trasladará al servicio o servicios de seguridad españoles competentes que deberán dar oportuna respuesta en tiempo y forma con arreglo a lo dispuesto en el artículo 10 de esta Ley.

7. El servicio español de seguridad competente que facilite información e inteligencia de conformidad con la presente Ley podrá, de acuerdo con la legislación nacional, imponer condiciones para el uso de la información e inteligencia al servicio de seguridad competente destinatario. También podrá imponer condiciones relativas a la notificación de los resultados de la investigación criminal o de la operación de inteligencia criminal en cuyo contexto se haya producido el intercambio de información e inteligencia.

Artículo 10. Plazos para el suministro de información e inteligencia.

1. El servicio de seguridad español competente previsto en la disposición adicional primera de esta Ley deberá responder en el plazo máximo de ocho horas a las solicitudes urgentes de información e inteligencia relativas a delitos enumerados en el apartado primero del artículo 9 de la Ley 3/2003, de 14 de marzo, sobre la orden europea de

detención y entrega, cuando la información o inteligencia solicitada se encuentre en una base de datos a la que tenga acceso directo un servicio español de seguridad.

2. En el caso de que el servicio de seguridad competente requerido no pueda responder en el plazo de ocho horas, comunicará los motivos por medio del formulario cuyo modelo se aprobará por el Ministro del Interior. Si el suministro de la información o inteligencia solicitadas dentro del plazo de ocho horas supone una carga desproporcionada para el servicio de seguridad competente requerido, éste podrá aplazar dicho suministro. En tal caso, deberá informar inmediatamente al servicio de seguridad competente requirente de tal aplazamiento y proporcionarle la información o inteligencia solicitada lo antes posible y, a más tardar, en un plazo de tres días.

3. Las solicitudes no urgentes de información e inteligencia relativas a los delitos enumerados en el apartado primero del artículo 9 de la Ley 3/2003, de 14 de marzo, se responderán en el plazo de una semana siempre que la información o inteligencia solicitada se encuentre en una base de datos a la que el servicio de seguridad español competente tenga acceso directo. En caso de que el servicio de seguridad español competente requerido no pueda responder en el plazo de una semana, comunicará los motivos por medio del formulario cuyo modelo se aprobará por el Ministro del Interior.

En todos los demás casos, el servicio de seguridad español competente velará porque la información solicitada por el servicio de seguridad competente de otro Estado miembro se comunique en el plazo de catorce días. En caso de que el servicio de seguridad competente requerido no pueda responder en el plazo de catorce días, comunicará los motivos por medio del formulario cuyo modelo se aprobará por el Ministro del Interior.

Artículo 11. *Motivos para no comunicar información o inteligencia.*

1. Sin perjuicio de lo dispuesto en el apartado tercero del artículo 9 de esta Ley, los servicios españoles de seguridad competentes sólo podrán negarse a facilitar información o inteligencia cuando concurren razones de hecho que hagan suponer que el suministro de la información o inteligencia:

- a) Pudiera perjudicar intereses esenciales en materia de seguridad nacional del Estado español.
- b) Pudiera comprometer el éxito de una investigación en curso o de una operación de inteligencia criminal o la seguridad de las personas.
- c) Fuera claramente desproporcionado o irrelevante para el fin que persigue la solicitud.

2. Cuando la solicitud se refiera a un delito castigado con pena de prisión igual o inferior a un año con arreglo a la legislación penal española, el servicio español de seguridad competente podrá negarse a facilitar la información o inteligencia requerida.

3. El servicio de seguridad competente se negará a facilitar la información o inteligencia solicitadas si la Autoridad judicial competente no ha autorizado el acceso y el intercambio de la información e inteligencia solicitada, con arreglo a lo previsto en el apartado cuarto del artículo 9 de la presente Ley.

Artículo 12. *Remisión de oficio por parte del Reino de España de información e inteligencia.*

1. No obstante lo dispuesto en el artículo 11 de esta Ley y sin necesidad de solicitud previa, el servicio español de seguridad competente remitirá de oficio a los servicios de seguridad competentes de los demás Estados miembros, cuando haya razones de hecho para creer que esa información e inteligencia pueden ayudar al descubrimiento, la prevención o la investigación de delitos enumerados en el apartado primero del artículo 9 de la Ley 3/2003, de 14 de marzo. Las modalidades de esta remisión de oficio se regirán por la legislación española.

2. La remisión de oficio de información e inteligencia se limitará a lo que se considere pertinente y necesario para el descubrimiento, prevención o investigación satisfactorios del delito o actividad delictiva de que se trate.

Disposición adicional primera. *Servicios de seguridad competentes y punto o puntos de contacto nacionales.*

1. A los efectos previstos en el artículo 3 de la presente Ley, los Ministerios del Interior y de Economía y Hacienda, en su ámbito respectivo de competencias, remitirán a la Secretaría General del Consejo, para su depósito, la declaración como «servicios de seguridad competentes» de las Fuerzas y Cuerpos de Seguridad del Estado, los Cuerpos de Policía de las Comunidades Autónomas y el Servicio de Vigilancia Aduanera. Esta declaración podrá modificarse en cualquier momento por el mismo procedimiento descrito anteriormente.

2. El Ministerio del Interior remitirá a la Secretaría General del Consejo la declaración de la Secretaría de Estado de Seguridad de dicho Ministerio como punto de conexión a los efectos del apartado sexto del artículo noveno de esta Ley. Esta declaración podrá ser modificada en los términos y condiciones que reglamentariamente se determinen y se remitirá a la Secretaría General del Consejo.

El Ministerio de Economía y Hacienda, en el ámbito de sus competencias, remitirá a la Secretaría General del Consejo la declaración donde se designe el servicio o servicios de seguridad que actuarán como punto o puntos de contacto nacionales a los efectos previstos en el apartado sexto del artículo 9 de esta Ley. Esta declaración podrá ser modificada en cualquier momento por una ulterior declaración que también deberá ser remitida a la Secretaría General del Consejo.

Disposición adicional segunda. *Autoridades judiciales competentes.*

1. A los efectos de lo previsto en el apartado cuarto del artículo 9 de la presente Ley, cuando la información solicitada forme parte de una investigación desarrollada en el seno de un procedimiento judicial abierto, el órgano jurisdiccional competente para autorizar o, en su caso, denegar el acceso, será el mismo que esté conociendo de dicho procedimiento.

2. A los mismos efectos de lo previsto en el precepto mencionado en el apartado anterior, cuando se requiera de autorización judicial para el acceso a la información solicitada los órganos jurisdiccionales competentes para autorizar o, en su caso, denegar dicho acceso, serán los Juzgados Centrales de Instrucción de la Audiencia Nacional.

3. Los órganos jurisdiccionales competentes, en todo caso, deberán resolver de forma expresa y en los mismos plazos que el artículo 10 de la presente ley fija a los servicios de seguridad.

Disposición adicional tercera. *Aplicación a Islandia, Noruega, Suiza y otros Estados que se adhieran al Acervo de Schengen.*

1. Lo dispuesto en esta Ley será también de aplicación con respecto a La República de Islandia, el Reino de Noruega y la Confederación Suiza.

2. Asimismo, la presente Ley será también de aplicación a aquellos Estados que suscriban con la Unión Europea el correspondiente Acuerdo de asociación para la ejecución, aplicación y desarrollo del Acervo de Schengen.

Disposición final primera. *Desarrollo reglamentario.*

1. Se habilita al Gobierno para que pueda desarrollar reglamentariamente las disposiciones contenidas en la presente Ley.

2. Se habilita al Ministro del Interior para aprobar los formularios relativos a las solicitudes de información e inteligencia, así como a su transmisión o denegación, previstas en esta Ley.

Disposición final segunda. *Habilitación competencial.*

La presente Ley se dicta en ejercicio de las competencias atribuidas al Estado en materia de seguridad pública por el artículo 149.1.29.^a de la Constitución.

Disposición final tercera. *Incorporación de Derecho de la Unión Europea.*

Mediante esta Ley se incorpora al Derecho Español la Decisión Marco del Consejo 2006/960/JAI, de 18 de diciembre, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea.

Disposición final cuarta. *Entrada en vigor.*

La presente Ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Por tanto,
Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta ley.

Madrid, 27 de julio de 2010.

JUAN CARLOS R.

El Presidente del Gobierno,
JOSÉ LUIS RODRÍGUEZ ZAPATERO

I. DISPOSICIONES GENERALES

JEFATURA DEL ESTADO

12133 *Ley Orgánica 6/2010, de 27 de julio, complementaria de la Ley 31/2010, de 27 de julio, sobre simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.*

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica:

PREÁMBULO

La Ley sobre simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea establece, en su disposición adicional segunda, apartado segundo, que, cuando se requiera de autorización judicial para el acceso a la información solicitada, los órganos jurisdiccionales competentes para autorizar o, en su caso, denegar dicho acceso serán los Juzgados Centrales de Instrucción de la Audiencia Nacional, salvo que la información forme parte de un procedimiento judicial abierto, en cuyo caso el competente a tal fin será el órgano judicial que esté conociendo de dicho procedimiento.

En consecuencia, debe darse una nueva redacción al artículo 88 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, que asigne a los Juzgados Centrales de Instrucción la competencia para autorizar o, en su caso, denegar, cuando se requiera autorización judicial, el acceso a la información solicitada en el marco de la Ley citada en el párrafo anterior, siempre que la información solicitada no forme parte de una investigación desarrollada en el seno de un procedimiento judicial abierto, en cuyo caso la competencia corresponderá al órgano jurisdiccional que esté conociendo de dicho procedimiento.

Artículo único. *Modificación del artículo 88 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.*

El artículo 88 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, queda redactado de la siguiente forma:

«En la villa de Madrid podrá haber uno o más Juzgados Centrales de Instrucción, con jurisdicción en toda España, que instruirán las causas cuyo enjuiciamiento corresponda a la Sala de lo Penal de la Audiencia Nacional o, en su caso, a los Juzgados Centrales de lo Penal y que tramitarán los expedientes de ejecución de las órdenes europeas de detención y entrega, y de extradición pasiva, así como las solicitudes de información entre los servicios de seguridad de los Estados miembros de la Unión Europea cuando requieran autorización judicial, en los términos previstos en la Ley.»

Disposición final primera. *Competencia estatal.*

Esta Ley Orgánica se dicta en ejercicio de las competencias atribuidas al Estado en materia de legislación procesal por el artículo 149.1.6.^ª de la Constitución.

Disposición final segunda. *Entrada en vigor.*

La presente Ley Orgánica entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Por tanto,
Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta ley orgánica.

Madrid, 27 de julio de 2010.

JUAN CARLOS R.

El Presidente del Gobierno,
JOSÉ LUIS RODRÍGUEZ ZAPATERO