LEY ORGÁNICA 15/91999, 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, solo 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 rectificados 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 prohibe 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 tránsito, 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 aquél a quien se pretenden comunicar.

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

5. Aquél 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 podrá 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 rectificados o cancelados, 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 rectificados 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 PRIMERO

Ficheros de titularidad pública

ARTÍCULO 20. CREACIÓN, MODIFICACIÓN O SUPRESIÓN

1. La creación, modificación o supresión de los ficheros de las Adminis traciones Públicas sólo podrán hacerse por medio de disposición general publicada en el “Boletín Oficial del Estado” o diario oficial correspondiente.

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

a) La finalidad del fichero y los usos previstos para el mismo.
b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
c) El procedimiento de recogida de los datos de carácter personal.
d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
f) Los órganos de las Administraciones responsables del fichero.
g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

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

ARTÍCULO 21. COMUNICACIÓN DE DATOS ENTRE ADMINISTRACIONES PÚBLICAS

1. Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra.
3. No obstante lo establecido en el artículo 11.2 b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una Ley prevea otra cosa.
4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

ARTÍCULO 22. FICHEROS DE LAS FUERZAS Y CUERPOS DE SEGURIDAD

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

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

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

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

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

ARTÍCULO 23. EXCEPCIONES A LOS DERECHOS DE ACCESO, RECTIFICACIÓN Y CANCELACIÓN

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

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

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

ARTÍCULO 24. OTRAS EXCEPCIONES A LOS DERECHOS DE LOS AFECTADOS

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

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

CAPÍTULO II

Ficheros de titularidad privada

ARTÍCULO 25. CREACIÓN

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

ARTÍCULO 26. NOTIFICACIÓN E INSCRIPCIÓN REGISTRAL

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

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

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

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

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

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

ARTÍCULO 27. COMUNICACIÓN DE LA CESIÓN DE DATOS

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

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

ARTÍCULO 28. DATOS INCLUIDOS EN LAS FUENTES DE ACCESO PÚBLICO

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

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

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

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

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

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

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

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

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

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 de 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 aquélla 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 aquéllas 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 Ge neral 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 de 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 foma 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 inmediantamente 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.

DISPOSICIONES ADICIONALES

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 deberá 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.

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.

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 50 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.

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.

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.

Sexta. Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados.

Se modifica el artículo 24.3, párrafo 2º 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".

DISPOSICIONES TRANSITORIAS

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.

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.

Tercera. Subsistencia de normas preexistentes.

Hasta tanto se lleven a efecto 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

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

DISPOSICIONES FINALES

Primera. Habilitación para el desarrollo reglamentario

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

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.

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.

Real Decreto 1332/94 de 20 de junio por el que se desarrollan algunos preceptos de la Ley Orgánica.

MINISTERIO DE JUSTICIA E INTERIOR

REAL DECRETO 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, habilita al Gobierno, en su disposición final primera, para dictar las disposiciones necesarias para la aplicación y desarrollo de la referida Ley, a la par que contiene en diferentes preceptos unos concretos mandatos al Gobierno para que por vía reglamentaria regule determinados aspectos, en su mayoría de orden procedimental, referentes al ejercicio de los derechos de acceso, rectificación y cancelación, a la forma de reclamar ante la Agencia de Protección de Datos por actuaciones contrarias a la Ley, a la notificación e inscripción de los ficheros automatizados de datos y al procedimiento para la determinación de las infracciones y la imposición de las sanciones.

En uso de dicha habilitación, y cumplimentando el mandato conferido en los artículos 15.1, 16.1, 17.1, 24.2, 38.3, y 47.1 de la citada Ley Orgánica, se dicta la presente disposición.

En su virtud, a propuesta del Ministro de Justicia e Interior, con la aprobación del Ministro para las Administraciones Públicas, previo informe de la Agencia de Protección de Datos, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 17 de junio de 1994.

DISPONGO:

CAPÍTULO I: Disposiciones Generales.

Artículo 1. Definiciones.

A efectos de lo dispuesto en el presente Real Decreto se entenderá por:

Bloqueo de datos: la identificación y reserva de datos con el fin de impedir su tratamiento.

Cesión de datos: toda obtención de datos resultante de la consulta de un fichero, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta de la afectada.

Datos accesibles al público: los datos que se encuentran a disposición del público en general, no impedida por cualquier norma limitativa, y están recogidos en medios tales como censos, anuarios, bases de datos públicas, repertorios de jurisprudencia, archivos de prensa, repertorios telefónicos o análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo.

Datos de carácter personal: toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

Identificación del afectado: cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada.

Transferencia de datos: el transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional.

Artículo 2.Regímenes especiales.

De conformidad con lo dispuesto en el artículo 2.3 de la Ley Orgánica 5/1992 se regirán por las disposiciones que, en materia de protección de datos, contienen las leyes y reglamentos respectivos, los ficheros siguientes:

El censo electoral, el fichero de electores y ficheros complementarios, regulados por la legislación de régimen electoral.

Los ficheros automatizados creados con fines exclusivamente estadísticos y amparados en cuanto a protección de datos por la normativa reguladora de la función estadística pública, sin perjuicio de lo prevenido en el artículo 36, m) de la Ley Orgánica 5/1992.

Los ficheros automatizados de estado civil, amparados por la Ley del Registro Civil y su Reglamento.

Los ficheros automatizados de antecedentes penales.

Los ficheros automatizados creados o gestionados al amparo de la normativa sobre protección de materias clasificadas.

Los ficheros automatizados cuyo objeto sea el almacenamiento de los datos contenidos en los informes personales regulados en el artículo 68 de la Ley 17/1989, de 19 de julio, reguladora del Régimen del personal militar profesional.

La remisión al Derecho nacional, contenida en los Títulos IV y VI del Convenio de 19 de junio de 1990, de aplicación del Acuerdo de Schengen de 14 de junio de 1985, así como cualquier otra remisión hecha a disposiciones nacionales de protección de datos personales contenida en convenios internacionales, se entenderá referida a la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, y a las disposiciones reglamentarias de desarrollo.

CAPÍTULO II: Transferencia internacional de datos.

Artículo 3.Régimen de las transferencias.

Si la transferencia de los datos de carácter personal tuviera como destinatario un país que no proporciona un nivel de protección equiparable al que presta la Ley Orgánica 5/1992, el Director de la Agencia de Protección de Datos autorizará la transferencia de los mismos, siempre que el cedente de los datos acredite haber cumplido lo dispuesto en los preceptos de la referida Ley y otorgue las garantías que al efecto le sean exigidas. A tal fin, la autorización deberá ser sometida al cumplimiento de las condiciones o cargas modales que se consideren necesarias para que de la transferencia no se deriven perjuicios a los derechos de los afectados y se respeten los principios contenidos en el Título II de la Ley Orgánica 5/1992.

En caso de incumplimiento de los términos de la autorización el cedente y el cesionario de los datos responderán solidariamente a efectos de lo previsto en el artículo 17.3 de la Ley Orgánica 5/1992.

Artículo 4.Excepciones.

Se exceptúan, en todo caso, de la autorización previa del Director de la Agencia de Protección de Datos las transferencias de datos de carácter personal que resulten de la aplicación de tratados o convenios de los que sea parte España y, en particular:

-Las transmisiones de datos registrados en ficheros creados por las Fuerzas y Cuerpos de Seguridad en función de una investigación concreta, hechas por conducto Interpola u otras vías previstas en convenios en los que España sea parte, cuando las necesidades de la investigación en curso exijan la transmisión a servicios policiales de otros Estados.

-Las transmisiones de datos registrados en la parte nacional española del Sistema de Información Schengen, con destino a la unidad de apoyo del sistema, a los solos efectos de una investigación policial en curso que requiera la utilización de datos del sistema. Las transmisiones de datos previstas en el sistema de intercambios de información contemplado en el Título VI del Tratado de la Unión Europea.

-Las transmisiones de los datos registrados en los ficheros creados por las Administraciones tributarias, en favor de los demás Estados miembros de la Unión Europea o en favor de otros Estados terceros, en virtud de lo dispuesto en los convenios internacionales de asistencia mutua en materia tributaria.

Se exceptúan, asimismo, de la autorización previa del Director de la Agencia de Protección de Datos, cualquiera que sea el Estado destinatario de los datos, las transmisiones de datos que se efectúen para cumplimentar exhortas, cartas órdenes, comisiones rotatorias u otras peticiones de auxilio judicial internacional, y los demás supuestos previstos en el artículo 33 de la Ley Orgánica 5/1992.

CAPÍTULO III: Notificacion e inscripción de ficheros.

Artículo 5.Notificación de ficheros de titularidad pública.

Todo fichero de datos de carácter personal, de titularidad pública, será notificado a la Agencia de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, mediante el traslado, a través del modelo normalizado que al efecto elabore la Agencia, de una copia de la disposición de creación del fichero.

Artículo 6.Notificación de ficheros de titularidad privada.

La persona o entidad que pretenda crear un fichero de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos mediante escrito o soporte informático en modelo normalizado que al efecto elabore la Agencia, en el que se especificarán los siguientes extremos:

1.- Nombre, denominación o razón social, documento nacional de identidad o código de identificación fiscal, dirección y actividad u objeto social del responsable del fichero.
2.- Ubicación del fichero.
3.- Identificación de los datos que se pretendan tratar, individualizando los supuestos de datos especialmente protegidos.
4.- Dirección de la oficina o dependencia en la cual puedan ejercerse los derechos de acceso, rectificación y cancelación.
5.- Origen o procedencia de los datos.
6.- Finalidad del fichero.
7.- Cesiones de datos previstas.
8.- Transferencias temporales o definitivas que se prevean realizar a otros países, con expresión de los mismos.
9.- Destinatarios o usuarios previstos para las cesiones o transferencias.
10.- Sistemas de tratamiento automatizado que se vayan a utilizar.
11.- Medidas de seguridad.

Artículo 7.Inscripción de los ficheros.

1.-Los ficheros de titularidad pública serán inscritos de oficio por la Agencia de Protección de Datos, una vez haya recibido la copia de la disposición de creación del fichero.

2.-El Director de la Agencia de Protección de Datos, a propuesta del Registro General de Protección de Datos, acordará la inscripción de los ficheros de titularidad privada si la notificación contuviera la información preceptiva y se cumplen las restantes exigencias legales, requiriendo, en caso contrario, al responsable del fichero para que la complete o subsane en el plazo de diez días, con indicación de que, si así no lo hiciera, se le tendrá por desistido de su petición, archivándose sin más trámite.

3.-La inscripción contendrá, en el supuesto de ficheros de titularidad pública, las indicaciones previstas en el artículo 18.2 de la Ley Orgánica 5/1992, con especificación de la disposición general de creación y del diario oficial de su publicación, y, en el supuesto de ficheros de titularidad privada, los extremos relacionados en el artículo 6 del presente Real Decreto, con excepción de las medidas de seguridad.

4.-La inscripción será notificada al responsable del fichero por el Registro General de Protección de Datos.

Artículo 8. Modificación y cancelación de la inscripción.

1.-La modificación o, en su caso, cancelación de la inscripción de los ficheros de titularidad pública se producirá de oficio por la Agencia de Protección de Datos, previo traslado por el órgano de la Administración responsable del fichero de una copia de la disposición general que modifique o suprima aquél.

2.-Cuando se trata de ficheros de titularidad privada, cualquier modificación posterior en el contenido de los extremos a que se refiere el artículo 6 del presente Real Decreto se comunicará, a efectos de inscripción, en su caso, a la Agencia de Protección de Datos dentro del mes siguiente a la fecha en que aquélla se hubiera producido. En igual plazo se comunicará la decisión de supresión del fichero a efectos de la cancelación del correspondiente asiento de inscripción.

Artículo 9.Inscripción y publicidad de los códigos tipo.

1.-Los códigos tipo se depositarán, para su inscripción, en el Registro General de Protección de Datos.
2.-El Director de la Agencia de Protección de Datos podrá denegar la inscripción si el código tipo no se ajusta a las disposiciones de la Ley Orgánica 5/1992 y del presente Real Decreto, sin perjuicio de requerir a los solicitantes para que subsanen las deficiencias.
3.-Los particulares podrán obtener copias de los códigos tipo depositados e inscritos en el Registro General de Protección de Datos.
4.-En caso de incumplimiento de las normas contenidas en los códigos tipo se estará a lo dispuesto al efecto en los acuerdos o decisiones que los formulen.

Artículo 10.Recursos.

Contra las resoluciones del Director de la Agencia de Protección de Datos relativas a la inscripción o, en su caso, a la modificación o cancelación de la inscripción de un fichero o código tipo, procederá el recurso contencioso-administrativo.

CAPÍTULO IV: Ejercicio y tutela de los derechos del afectado

Artículo 11.Carácter personal de los derechos.

Los derechos de acceso a los ficheros automatizados, así como los de rectificación y cancelación de datos son personalísimos y serán ejercidos por el afectado frente al responsable del fichero, sin otras limitaciones que las que prevén la Ley Orgánica 5/1992 y el presente Real Decreto.

Podrá, no obstante, actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos.

Artículo 12.Derecho de acceso.

El derecho de acceso se ejercerá mediante petición o solicitud dirigida al responsable del fichero, formulada por cualquier medio que garantice la identificación del afectado y en la que conste el fichero o ficheros a consultar.

El afectado podrá optar por uno o varios de los siguientes sistemas de consulta del fichero, siempre que la configuración e implantación material del fichero lo permita:

-Visualización en pantalla.
-Escrito, copia o fotocopia remitida por correo.
-Telecopia.

Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del mismo.

El responsable del fichero resolverá entre la petición de acceso en el plazo máximo de un mes, a contar de la recepción de la solicitud. Transcurrido este plazo sin que de forma expresa se responda a la petición de

acceso, éste podrá entenderse desestimada a los efectos de la interposición de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992.

Si la resolución fuera estimatoria, el acceso se hará efectivo en el plazo de los diez días siguientes a la notificación de aquélla.

Artículo 13.Contenido de la información.

La información, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, previa transcripción en claro de los datos del fichero, en su caso.

La información comprenderá los datos de base del afectado y los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

Artículo 14.Denegación del acceso.

Se denegará el acceso a los datos de carácter personal registrados en ficheros de titularidad pública cuando se dé alguno de los supuestos contemplados e los artículos 14.3, 21.1 y 2 y 22.2 de la Ley Orgánica 5/1992.

Tratándose de datos de carácter personal registrados en ficheros de titularidad privada, únicamente se denegará el acceso cuando la solicitud sea formulada por persona distinta del afectado.

Artículo 15.Denegación del acceso.

Cuando el acceso a los ficheros revelare que los datos del afectado son inexactos o incompletos, inadecuados o excesivos, podrá éste solicitar del responsable del fichero la rectificación o, en su caso, cancelación de los mismos.

No obstante, cuando se trate de datos que reflejen hechos constatados en un procedimiento administrativo, aquéllos se considerarán exactos siempre que coincidan con éste.

La rectificación o cancelación se hará efectiva por el responsable del fichero dentro de los cinco días siguientes al de la recepción de la solicitud. En idéntico plazo se efectuará la notificación a que se refiere el artículo 15.3 de la Ley Orgánica 5/1992.

En el supuesto de que el responsable del fichero considere que no procede acceder a lo solicitado por el afectado, se lo comunicará motivadamente y dentro del plazo señalado en el apartado anterior, a fin de que por éste se pueda hacer uso de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992.

Transcurrido el plazo previsto en el apartado 2 sin que de forma expresa se responda a la solicitud de rectificación o cancelación, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación que corresponda.

Artículo 16.Bloqueo de los datos.

En los casos en que, siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, el responsable del fichero procederá al bloqueo de los datos, con el fin de impedir su ulterior proceso o utilización.

Se exceptúa, no obstante, el supuesto de que se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren.

Contra la resolución por la que el responsable del fichero acuerde el bloqueo de los datos procederá reclamación ante el Director de la Agencia de Protección de Datos.

Artículo 17.Tutela de los derechos.

Las reclamaciones de los afectados ante la Agencia de Protección de Datos, a que se refiere el artículo 17.1 de la Ley Orgánica 5/1992, se sustanciarán en la forma prevista en el presente artículo.

El procedimiento se iniciará a instancia del afectado o afectados, expresando con claridad el contenido de su reclamación y de los preceptos de la Ley Orgánica 5/1992 que se consideran vulnerados.

Recibida la reclamación en la Agencia de Protección de Datos, se dará traslado de la misma al responsable del fichero, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.

Recibidas las alegaciones o transcurrido el plazo previsto en el apartado anterior, la Agencia de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada, dando traslado de la misma a los interesados.

Contra la resolución del Director procederá recurso contencioso-administrativo.

CAPÍTULO V: Procedimiento sancionador.

Artículo 18.Iniciación e instrucción.

El procedimiento sancionador previsto en el artículo 47 de la Ley Orgánica 5/1992, se iniciará siempre de oficio, bien por propia iniciativa o en virtud de denuncia de un afectado o afectados, por acuerdo del Director de la Agencia de Protección de Datos, en el cual se designará instructor y, en su caso, secretario, con expresa indicación del régimen de recusación de los mismos.

En el referido acuerdo se identificará a la persona o personas presuntamente responsables y se concretarán los hechos imputados, con expresión de la infracción presuntamente cometida y de la sanción o sanciones que pudieran imponerse, así como de las medidas provisionales que, en su caso, se adopten.

El acuerdo de incoación del expediente se notificará al presunto responsable y en el mismo se informará a éste de su derecho a formular alegaciones y utilizar los medios de defensa procedentes y que la autoridad competente para imponer, en su caso, la sanción es el Director de la Agencia de Protección de Datos, con cita expresa del presente artículo y del artículo 36, g) en relación con el artículo 35, ambos de la Ley Orgánica 5/1992.Dentro de los quince días siguientes a la notificación del acuerdo de incoación, el instructor ordenará, de oficio, la práctica de cuantas pruebas y actos de instrucción sean adecuados para esclarecer los hechos y determinar las responsabilidades susceptibles de sanción. En idéntico plazo, el presunto responsable podrá formular las alegaciones y proponer las pruebas que considere convenientes.

Transcurrido el plazo previsto en el apartado anterior, el instructor acordará la práctica de las pruebas que estime pertinentes, a cuyo efecto concederá un plazo de treinta días, transcurrido el cual el expediente se pondrá de manifiesto al presunto responsable para que, en el plazo de quince días, formule alegaciones y aporte cuantos documentos estime de interés.

Artículo 19.Resolución.

Cumplimentados los trámites previstos en el artículo anterior, el instructor formulará propuesta de resolución motivada en la cual se fijarán de modo claro y preciso los hechos, se razonará, en su caso, la denegación y de la práctica probatoria propuesta por el presunto responsable, se valorarán jurídicamente aquéllos a fin de determinar la infracción cometida y se señalará la sanción a imponer, determinando su cuantía con arreglo a los criterios establecidos en el artículo 44.4 de la Ley Orgánica 5/1992, o bien, se propondrá la declaración de no existencia de responsabilidad.

La propuesta de resolución se notificará al presunto responsable para que, en el plazo de quince días, pueda formular nuevas alegaciones si lo considera oportuno. Notificada la propuesta de resolución o expirado el plazo de alegaciones previsto en el apartado anterior, el instructor elevará el expediente completo al Director de la Agencia de Protección de Datos.

El Director podrá, antes de dictar resolución, ordenar al instructor la práctica de cuantas actuaciones considere necesarias, lo que se llevará a efecto en un plazo máximo de quince días.

La resolución, que se dictará dentro de los diez días siguientes, determinará con la necesaria precisión los hechos imputados, la infracción cometida, con expresión del precepto que la tipifique, el responsable de la misma y la sanción impuesta; o bien, la declaración de no existencia de responsabilidad. Contendrá,

asimismo, la declaración pertinente en orden a las medidas provisionales adoptadas durante la tramitación del procedimiento.

La resolución se notificará al responsable con expresión de su derecho a interponer recurso contencioso-administrativo, el plazo de interposición, y el órgano ante el cual deba ser presentado.

Si el procedimiento se hubiera iniciado como consecuencia de denuncia de un afectado, la resolución deberá ser notificada al firmante de la misma.

DISPOSICIONES.

Disposición adicional primera:Comunicación de ficheros preexistentes

Los ficheros automatizados de datos de carácter personal que se hubiesen creado con posterioridad a la entrada en vigor de la Ley Orgánica 5/1992 y antes de la vigencia del presente Real Decreto se deberán comunicar a la Agencia de Protección de Datos antes del 31 de julio de 1994.

Disposición adicional segunda:Ficheros de las Comunidades Autónomas.

Corresponde a las Comunidades Autónomas, respecto de sus propios ficheros, la regulación del ejercicio y tutela de los derechos del afectado y del procedimiento sancionador en los términos y con los límites establecidos en la Ley Orgánica 5/1992 y de acuerdo con las normas del procedimiento administrador común.

Disposición adicional tercera:Ficheros de las Administraciones Tributarias.

Los ficheros creados por las Administraciones Tributarias para la gestión de los tributos que se les encomienden, se regirán por las disposiciones del presente Real Decreto y por las demás disposiciones reglamentarias que, en desarrollo y con sujeción a lo dispuesto en la Ley Orgánica 5/1992, específicamente se aprueben para los mismos.

Disposición final primera:Lista de países con equiparable protección.

Se faculta al Ministro de Justicia e Interior para que, previo informe del Director de la Agencia de Protección de Datos, apruebe la relación de países que, a efectos de lo dispuesto en el artículo 32 de la Ley Orgánica 5/1992, se entiende que proporcionan un nivel de protección equiparable al de dicha Ley.

Disposición final segunda:Entrada en vigor.

El presente Real Decreto entrará en vigor el día siguiente al de su publicación en el "Boletín Oficial del Estado".

Dado en Madrid a 20 de junio de 1994.

JUAN CARLOS R.
El Ministro de Justicia e Interior,
JUAN ALBERTO BELLOCH JULBE

INSTRUCCIÓN NÚMERO 1/1995, DE 1 DE MARZO, DE LA AGENCIA DE PROTECCIÓN DE DATOS, RELATIVA A PRESTACIÓN DE SERVICIOS DE INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO.

El artículo 36 de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, al definir las funciones de la Agencia de Protección de Datos, incluye en su apartado c) la de dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de dicha Ley. Disposición que tiene su complemento en el artículo 5. c) del Estatuto de la Agencia, aprobado por Real Decreto 428/1993, de 26 de marzo, que señala entre las funciones de la misma la de dictar las instrucciones y recomendaciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica.

El artículo 28 de la misma se refiere a la prestación de servicios de información sobre solvencia patrimonial y crédito desde una doble perspectiva. Por un lado, determina que quienes se dediquen a la prestación de servicios sobre la solvencia patrimonial y el crédito sólo podrán tratar automatizadamente datos de carácter personal obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento. Por otro, regula el tratamiento de datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias señalando que podrán tratarse dichos datos siempre que sean “facilitados por el acreedor o por quien actúe por su cuenta o interés”.

Los primeros no se apartan de la regulación común que establece la Ley Orgánica; los segundos presentan, por el contrario, un conjunto de especialidades, (excepción del principio del consentimiento tanto en la recogida del dato como en su tratamiento), que hacen necesario efectuar una serie de precisiones. Además, dentro de estos últimos, la realidad demuestra que coexisten perfectamente engarzados dos tipos de ficheros: uno, el propio del acreedor, que se nutre de los datos personales que son consecuencia de las relaciones económicas mantenidas con el afectado, cuya única finalidad es obtener la satisfacción de la obligación dineraria, y otro, un fichero que se podría denominar común que, consolidando todos los datos personales contenidos en aquellos otros ficheros, tiene por finalidad proporcionar información sobre la solvencia de una persona determinada y cuyo responsable, al no ser el acreedor, no tiene competencia para modificar o cancelar los datos inexactos que se encuentran en aquéllos.

En consecuencia, en uso de las facultades que tiene conferidas, la Agencia de Protección de Datos ha dispuesto:

CAPÍTULO PRIMERO

Calidad de los datos objetos del tratamiento automatizado, forma y veces en que debe efectuarse la notificación y cómputo del plazo al que se refiere el artículo 28.3 de la Ley Orgánica

NORMA PRIMERA

Calidad de los datos objeto de tratamiento

1. La inclusión de los datos de carácter personal en los ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias, a los que se refiere el artículo 28 de la Ley Orgánica 5/1992, deberá efectuarse solamente cuando concurran los siguientes requisitos:

a) Existencia previa de una deuda cierta, vencida y exigible, que haya resultado impagada.

b) Requerimiento previo de pago a quien corresponda, en su caso, el cumplimiento de la obligación.

2. No podrán incluirse en los ficheros de esta naturaleza datos personales sobre los que exista un principio de prueba documental que aparentemente contradiga alguno de los requisitos anteriores. Tal circunstancia determinará igualmente la desaparición cautelar del dato personal desfavorable en los supuestos en que ya se hubiera efectuado su inclusión en el fichero.

3. El acreedor o quien actúe por su cuenta e interés deberá asegurarse que concurren todos los requisitos exigidos en el número 1 de esta Norma en el momento de notificar los datos adversos al responsable del fichero común.

4. La comunicación del dato inexistente o inexacto, con el fin de obtener su cancelación o modificación, deberá efectuarse por el acreedor o quien actúe por su cuenta al responsable del fichero común en el mínimo tiempo posible, y en todo caso en una semana. Dicho plazo es independiente del establecido en el artículo 15.2 del Real Decreto 1332/1994, de 20 de junio, y que se aplica al fichero del acreedor.

NORMA SEGUNDA

Notificación de la inclusión en el fichero

1. La notificación de la inclusión de datos personales en el fichero efectuada con posterioridad a la entrada en vigor de la Ley Orgánica 5/1992 se efectuará en la forma establecida en el artículo 28 de la misma.

2. Cuando se trate de datos personales incorporados al fichero con anterioridad a la entrada en vigor de la Ley Orgánica deberán notificarse al afectado en el menor plazo posible y, en todo caso, dentro del año siguiente contado desde la publicación de la presente Instrucción.

3. La inscripción en el fichero de la obligación incumplida se efectuará, bien en un solo asiento si fuese de vencimiento único, bien en tantos asientos como vencimientos periódicos incumplidos existan señalando, en este caso, la fecha de cada uno de ellos.

4. Se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores.

5. El responsable del fichero deberá adoptar las medidas organizativas y técnicas necesarias que permitan acreditar la realización material del envío de notificación y la fecha de entrega o intento de entrega de la misma.

6. La notificación se dirigirá a la última dirección conocida del afectado a través de un medio fiable e independiente del responsable del fichero.

NORMA TERCERA

Cómputo del plazo de seis años que establece el artículo 28.3 de la Ley Orgánica

El cómputo del plazo a que se refiere el artículo 28.3 de la Ley Orgánica se iniciará a partir del momento de la inclusión del dato personal desfavorable en el fichero y, en todo caso, desde el cuarto mes, contado a partir del vencimiento de la obligación incumplida o del plazo en concreto de la misma si fuera de cumplimiento periódico.

CAPÍTULO SEGUNDO

Medidas de seguridad

NORMA CUARTA

Forma de comprobación

1. Los sistemas que almacenen o procesen información relativa al cumplimiento o incumplimiento de obligaciones dinerarias deberán acreditar la efectiva implantación de las medidas de seguridad exigidas por el artículo 9.1 de la Ley Orgánica dentro del año siguiente a la publicación de la presente Instrucción. Para los ficheros que se inscriban con posterioridad a esta Instrucción, el plazo se computará a partir de la fecha en que aquélla se haya efectuado en el Registro General de Protección de Datos.

2. La implantación, idoneidad y eficacia de dichas medidas se acreditará mediante la realización de una auditoría, proporcionada a la naturaleza, volumen y características de los datos personales almacenados y tratados, y la remisión del informe final de la misma a la Agencia de Protección de Datos.

3. La auditoría podrá ser realizada:

a) Por el departamento de auditoría interna del responsable del fichero, si cuenta con un departamento formalmente constituido, profesionalmente cualificado e independiente del órgano responsable del tratamiento y gestión de los datos.

b) Por un auditor externo, profesionalmente cualificado e independiente del responsable del fichero.

4. La auditoría deberá ser realizada de acuerdo con las normas y recomendaciones de ejercicio profesional aplicables en el momento de su ejecución.

5. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles destinados a garantizar la integridad y confidencialidad de los datos personales almacenados o tratados, identificar sus deficiencias o insuficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basan los dictámenes alcanzados y recomendaciones propuestas.

6. Adicionalmente, los sistemas que almacenen o procesen información relativa al cumplimiento o incumplimiento de obligaciones dinerarias deberán someterse a una nueva auditoría tras la adopción de las medidas específicas que, en su caso, la Agencia determine, a resultas del informe inicial de auditoría. En todo caso, dichos sistemas deberán ser auditados periódicamente, a intervalos no mayores de dos años.

NORMA FINAL

Entrada en vigor

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

Madrid, 1 de marzo de 1995.- El Director, Juan José Martín-Casallo López.

INSTRUCCIÓN NÚMERO 2/1995, DE 4 DE MAYO, DE LA AGENCIA DE PROTECCIÓN DE DATOS, SOBRE MEDIDAS QUE GARANTIZAN LA INTIMIDAD DE LOS DATOS PERSONALES RECABADOS COMO CONSECUENCIA DE LA CONTRATACIÓN DE UN SEGURO DE VIDA DE FORMA CONJUNTA CON LA CONCESIÓN DE UN PRÉSTAMO HIPOTECARIO O PERSONAL.

La concesión de un crédito hipotecario o personal, que suele ir acompañada de un seguro de vida por el importe de aquél y del que se señala como beneficiaria a la Entidad de crédito de que se trate por la suma del capital no amortizado, incide sobre un importante número de disposiciones de nuestro ordenamiento jurídico.

Es obvio que la regulación jurídica de alguna de estas materias, (Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios; Ley 16/1989, de 17 de julio, de Defensa de la Competencia; Ley 9/1992, de 30 de abril, de Mediación en Seguros Privados), excede de las competencias que tiene atribuidas la Agencia de Protección de Datos. Ahora bien, la precisión de si los datos son o no sensibles, con la incidencia que ello tiene en su recogida, tratamiento y cesión, la determinación del fichero en donde deban ser tratados, la de si es preciso que en esta materia, por tratarse de datos especialmente protegidos, el nivel de protección de los mismos se extienda excepcionalmente a los ficheros manuales o no automatizados, son, entre otras, cuestiones que deben ser fijadas por la Agencia de Protección de Datos.

En consecuencia, en uso de las facultades que tiene conferidas, la Agencia de Protección de Datos ha dispuesto:

Norma primera: Ámbito de aplicación.

La presente Instrucción será de aplicación a los datos personales solicitados por las Entidades de crédito con motivo de la celebración de un contrato de seguro de vida anejo a la concesión de un crédito hipotecario o personal.

Norma segunda: De la recogida de los datos.

1. La obtención de datos personales a efectos de la celebración de un contrato de seguro de vida, anejo a la concesión de un crédito hipotecario o personal, efectuada por las Entidades de crédito a través de cuestionarios u otros impresos deberá realizarse, en todo caso, mediante modelos separados para cada uno de los contratos a celebrar. En los formularios cuyo destinatario sean las Entidades bancarias no podrán recabarse en ningún caso datos relativos a la salud del solicitante.
2. Cualquiera que sea el modo de llevarse a efecto la recogida de datos de salud necesarios para la celebración del seguro de vida deberá constar expresamente el compromiso de la Entidad de crédito de que los datos obtenidos a tal fin solamente serán utilizados por la Entidad aseguradora. Las Entidades de crédito no podrán incluir los datos de salud en sus ficheros informatizados o en aquellos en los que almacenen datos de forma convencional.
3. En ningún caso se considerará, por la naturaleza de la información solicitada o por las circunstancias en que se recaba, que se puede prescindir del derecho de la información en la recogida de los datos previsto en la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Por tanto, será necesario informar previamente, en los formularios u otros impresos de recogida, de modo expreso, preciso e inequívoco:

   a) De la existencia de un fichero automatizado 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 y cancelación.

   e) De la identidad y dirección del responsable del fichero.

4. Cuando la recogida de datos personales a efectos de la celebración de un contrato de seguro de vida, anejo a la concesión de un crédito hipotecario o personal efectuada por las Entidades de crédito, se lleve a cabo por procedimientos distintos a los del formulario u otros impresos deberá informarse al afectado de los extremos previstos en el apartado tercero.

Norma tercera: *Consentimiento del afectado y tratamiento de los datos.*

El afectado deberá manifestar su consentimiento por separado para cada uno de los contratos y para el tratamiento distinto de la información que ambos conllevan.

Las Entidades de crédito solamente podrán tratar aquellos datos personales, no especialmente protegidos, que sean estrictamente necesarios para relacionar el contrato de préstamo con el contrato de seguro de vida celebrado como consecuencia de aquél o que estén justificados por la intervención de la Entidad de crédito como agente o tomador del contrato de seguro.

Norma cuarta: Cesión de los datos.

En ningún caso podrá considerarse que la cesión de cualquier clase de datos personales solicitados por la Entidad aseguradora a la de crédito, o viceversa, se halla amparada por lo establecido en el artículo 11.2.c) de la Ley Orgánica 5/1992.

Norma transitoria: *Aplicación a contratos celebrados con anterioridad*.

Los datos de salud correspondientes a los contratos de seguro de vida celebrados con anterioridad a la publicación de esta Instrucción, que se encuentren incluidos en ficheros de las Entidades de crédito, automatizados o no, deberán ser cancelados en el plazo de un mes, contado a partir de la entrada en vigor de la misma.

Norma final: Entrada en vigor.

La presente Instrucción entrará en vigor al día siguiente de su publicación en el “Boletín Oficial del Estado”.

Madrid, 4 de mayo de 1995.- El Director, Juan José Martín-Casallo López.

INSTRUCCIÓN 1/1996, DE 1 DE MARZO, DE LA AGENCIA DE PROTECCIÓN DE DATOS, SOBRE FICHEROS AUTOMATIZADOS ESTABLECIDOS CON LA FINALIDAD DE CONTROLAR EL ACCESO A LOS EDIFICIOS.

La necesidad de regular los ficheros automatizados establecidos para el control del acceso de las personas a los centros de trabajo o dependencias públicas, a donde se acude con la finalidad de efectuar actividades relacionadas con las propias del centro visitado, plantea problemas relacionados con la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, con mayor razón desde la aprobación de la Directiva europea 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. Estos problemas se concretan en la necesidad de regular los datos constituidos por sonido e imagen, como los de vigilancia por videocámara, y, en general, todos los recopilados en cumplimiento de las funciones de vigilancia, con la prestación del consentimiento necesario para ello, así como el período en que los mismos deban ser conservados y su posterior cancelación por haber dejado de ser necesarios o pertinentes para los fines para los que fueron recabados.

La Instrucción solamente se refiere al ámbito competencial propio de la Ley reguladora del tratamiento automatizado de datos personales y se dicta de conformidad con lo dispuesto en el artículo 36.c) de la misma que atribuye a la Agencia de Protección de Datos competencias en esta materia.

Norma primera.- *Ámbito de aplicación*.

1. La presente Instrucción regula los datos de carácter personal tratados de forma automatizada que son recabados por los servicios de seguridad con la finalidad de controlar el acceso a los edificios públicos y privados, así como a establecimientos, espectáculos, certámenes y convenciones.

2. A tales efectos, tendrá la consideración de dato personal cualquier información concerniente a personas físicas identificadas o identificables, debiendo entenderse comprendidos dentro de la misma el sonido y la imagen.

Norma segunda.- Responsable del fichero.

1. Tendrá la consideración de responsable del fichero la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo por cuya cuenta se efectúe la realización del servicio de seguridad. No obstante lo anterior, mediante el correspondiente contrato de prestación de servicios de seguridad, podrá tener la consideración de responsable del fichero la empresa que preste los servicios de aquélla naturaleza.
2. El responsable del fichero asumirá el cumplimiento de todas las obligaciones establecidas en la Ley Orgánica 5/1992 y, entre ellas, la de la inscripción del fichero en el Registro General de Protección de Datos.

Norma tercera.- *Recogida de datos.*

1. La recogida de datos efectuada para el cumplimiento de los fines a los que se refiere la presente Instrucción deberá realizarse de conformidad con lo establecido en el artículo 5 de la Ley Orgánica 5/1992, y, en concreto, deberá informarse de la existencia de un fichero automatizado, de la finalidad de la recogida de los datos, de los destinatarios de la información, del carácter obligatorio de su respuesta, de las consecuencias de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación o cancelación y de la identidad y dirección del responsable del fichero.

2. Los datos recogidos serán los estrictamente necesarios para cumplir la finalidad de controlar el acceso.

Norma cuarta.- *Utilización de los datos.*

Los datos personales así obtenidos no podrán ser utilizados para otros fines. Tampoco podrán ser objeto de cesión los datos así recabados fuera de los casos expresamente establecidos en la ley, salvo consentimiento del afectado.

Norma quinta.- *Cancelación de los datos.*

Los datos de carácter personal deberán ser destruidos cuando haya transcurrido el plazo de un mes, contado a partir del momento en que fueron recabados.

Norma sexta.- *Medidas de seguridad.*

El responsable del fichero garantizará la adopción de las medidas técnicas y organizativas necesarias para la seguridad de los datos y que impidan el acceso no autorizado a los ficheros creados para dichos fines.

Norma final.- *Entrada en vigor.*

La presente Instrucción entrará en vigor a partir de los tres meses de su publicación en el “Boletín Oficial del Estado”.

Madrid, 1 de marzo de 1996.- El Director, Juan José Martín-Casallo López.

INSTRUCCIÓN 2/1996, DE 1 DE MARZO, DE LA AGENCIA DE PROTECCIÓN DE DATOS, SOBRE FICHEROS AUTOMATIZADOS ESTABLECIDOS CON LA FINALIDAD DE CONTROLAR EL ACCESO A LOS CASINOS Y SALAS DE BINGO.

La necesidad de establecer la forma de llevar los ficheros automatizados utilizados para controlar la entrada en casinos y salas de bingo obliga a precisar una serie de criterios interpretativos que faciliten la aplicación de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, con mayor razón desde la aprobación de la Directiva europea 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. En concreto, es necesario regular el cumplimiento del deber de información al ciudadano en la recogida de datos personales, el consentimiento en la cesión de los datos así recabados en los supuestos en que la misma no debe efectuarse por causas legales, así como el plazo en que los datos deben ser cancelados por haber dejado de ser necesarios o pertinentes para los fines para los que se recabaron.

La Instrucción solamente se refiere al ámbito competencial propio de la Ley reguladora del tratamiento automatizado de datos personales y se dicta de conformidad con lo dispuesto en el artículo 36.c) de la misma que atribuye a la Agencia de Protección de Datos competencias en esta materia.

Norma primera.- *Ámbito de aplicación*.

1. La presente Instrucción regula los datos de carácter personal tratados de forma automatizada que son recabados con la finalidad de controlar el acceso por las sociedades explotadoras de casinos de juego o por cualquier empresa titular de una sala de bingo.

2. A tales efectos, tendrá la consideración de dato personal cualquier información concerniente a personas físicas identificadas o identificables, debiendo entenderse comprendidos dentro de la misma el sonido y la imagen.

Norma segunda.- Responsable del fichero.

1. Tendrá la consideración de responsable del fichero la sociedad explotadora del casino de juego o la empresa titular de la sala de bingo.
2. El responsable del fichero asumirá el cumplimiento de todas las obligaciones establecidas en la Ley Orgánica 5/1992 y, entre ellas, la de la inscripción del fichero en el Registro General de Protección de Datos.

Norma tercera.- *Recogida de datos*.

1. La recogida de datos efectuada para el cumplimiento de los fines a los que se refiere la presente Instrucción deberá realizarse de conformidad con lo establecido en el artículo 5 de la Ley Orgánica 5/1992, y, en concreto, deberá informarse de la existencia de un fichero automatizado, de la finalidad de la recogida de datos, de los destinatarios de la información, del carácter obligatorio de su respuesta, de las consecuencias de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación o cancelación y de la identidad y dirección del responsable del fichero.

2. No podrán recogerse más datos personales que aquéllos estrictamente necesarios para controlar el acceso, quedando, en todo caso, limitados a los que aparecen en el documento identificador exigido para la entrada.

Norma cuarta.- *Utilización de los datos.*

Los datos personales así obtenidos no podrán ser utilizados para otros fines. Tampoco podrán ser objeto de cesión los datos así recabados fuera de los casos expresamente establecidos en la ley, salvo consentimiento del afectado.

Norma quinta.- *Cancelación de los datos*.

Los datos de carácter personal deberán ser destruidos cuando haya transcurrido el plazo de seis meses, contado a partir de la fecha del último acceso.

Norma sexta.- *Medidas de seguridad.*

El responsable del fichero garantizará la adopción de las medidas técnicas y organizativas necesarias para la seguridad de los datos y que impidan el acceso no autorizado a los ficheros creados para dichos fines.

Norma final.- *Entrada en vigor*.

La presente Instrucción entrará en vigor a partir de los tres meses de su publicación en el "Boletín Oficial del Estado".

Madrid, 1 de marzo de 1996.- El Director, Juan José Martín-Casallo López.

INSTRUCCIÓN 1/1998, DE 19 DE ENERO, DE LA AGENCIA DE PROTECCIÓN DE DATOS, RELATIVA AL EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN Y CANCELACIÓN.

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal dedica los artículos 14 y siguientes a los derechos de acceso, rectificación y cancelación de los datos de carácter personal contenidos en ficheros automatizados. Dichos derechos se configuran como uno de los ejes fundamentales sobre los que se articula la protección del honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, en desarrollo de lo dispuesto en el artículo 18.4 de la Constitución Española.

El ejercicio de los derechos de acceso, rectificación y cancelación aparece regulado no sólo en la Ley Orgánica 5/1992, sino también en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos procedimentales de la citada Ley.

Al amparo de lo dispuesto en el artículo 36.c) de la Ley Orgánica 5/92 que atribuye al Director de la Agencia la función de "Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la presente Ley", se ha elaborado la presente Instrucción.

Esta Instrucción tiene por objeto aclarar las disposiciones relativas a los derechos de acceso, rectificación y cancelación, ya que las actuaciones practicadas por esta Agencia han puesto de manifiesto que en su aplicación se presentan problemas interpretativos y que es necesario precisar el ejercicio de estos derechos en relación con algunos ficheros que presentan características especiales. Para ello, la Instrucción recoge la regulación de dichos derechos de acuerdo con la Ley Orgánica 5/1992 y el Real Decreto 1332/1994, de 20 de junio, y realiza una interpretación unitaria de los preceptos teniendo en cuenta la totalidad de principios legales.

En las normas primera, segunda y tercera se detallan los requisitos que deben cumplirse en el ejercicio de los derechos de acceso, rectificación y cancelación con carácter general. Sin embargo, las particularidades que presentan los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito y los ficheros con fines de publicidad exigen tratarlos de un modo especial en las normas cuarta y quinta, respectivamente.

NORMA PRIMERA. REQUISITOS GENERALES

1.- Los derechos de acceso a los ficheros automatizados, así como los de rectificación y cancelación de datos son personalísimos, y serán ejercidos por el afectado frente al responsable del fichero por lo que será necesario que el afectado acredite su identidad frente a dicho responsable. Estos

derechos se ejercerán sin otras limitaciones que las que prevén la Ley Orgánica 5/1992 y el Real Decreto 1332/1994, de 20 de junio.

Podrá, no obstante, actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos, en cuyo caso será necesario que el representante legal acredite tal condición.

2.- La Ley configura los derechos de acceso, rectificación y cancelación como derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

3.- El ejercicio de los derechos deberá llevarse a cabo mediante solicitud dirigida al responsable del fichero, que contendrá:

- Nombre, apellidos del interesado y fotocopia del DNI del interesado y, en los casos que excepcionalmente se admita, de la persona que lo represente, así como el documento acreditativo de tal representación. La fotocopia del DNI podrá ser sustituida siempre que se acredite la identidad por cualquier otro medio válido en derecho.

- Petición en que se concreta la solicitud.

- Domicilio a efectos de notificaciones, fecha y firma del solicitante.

- Documentos acreditativos de la petición que formula, en su caso.

El interesado deberá utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud.

4.- El responsable del fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción.

En el caso de que la solicitud no reúna los requisitos especificados en el apartado tercero, el responsable del fichero deberá solicitar la subsanación de los mismos.

5.- El responsable del fichero deberá adoptar las medidas oportunas para garantizar que todas las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

NORMA SEGUNDA. DERECHO DE ACCESO

1.- El afectado tiene derecho a solicitar y obtener información de sus datos de carácter personal incluidos en ficheros automatizados.

2.- Al ejercitar el derecho de acceso, el afectado podrá optar por uno o varios de los siguientes sistemas de consulta del fichero, siempre que la configuración o implantación material del fichero lo permita:

a) Visualización en pantalla

b) Escrito, copia o fotocopia remitida por correo

c) Telecopia

d) Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del mismo.

3.- El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes, a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, ésta podrá

entenderse desestimada a los efectos de la interposición de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

4.- Si la resolución fuera estimatoria, el acceso se hará efectivo en el plazo de los diez días siguientes a la notificación de aquella.

5.- El responsable del fichero podrá denegar el acceso a los datos de carácter personal cuando el derecho se haya ejercitado en un intervalo inferior a doce meses y no se acredite un interés legítimo al efecto, así como cuando la solicitud sea formulada por persona distinta del afectado.

Tratándose de ficheros de titularidad pública se podrá denegar el acceso en los supuestos de los artículos 21.1 y 21.2 de la Ley Orgánica 5/1992, en los que se establecen excepciones relativas a los

ficheros de las Fuerzas y Cuerpos de Seguridad del Estado y a los ficheros de la Hacienda Pública y del artículo 22 de la Ley Orgánica 5/1992.

6.- La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, previa transcripción en claro de los datos del fichero, en su caso, y comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

En el caso de que los datos provengan de fuentes diversas, deberán especificarse las mismas identificando la información que proviene de cada una de ellas.

NORMA TERCERA. DERECHOS DE RECTIFICACIÓN Y CANCELACIÓN.

1.- Si los datos de carácter personal del afectado son inexactos o incompletos, inadecuados o excesivos, podrá éste solicitar del responsable del fichero la rectificación o, en su caso, la cancelación de los mismos.

2.- Los derechos de rectificación y cancelación se harán efectivos por el responsable del fichero dentro de los cinco días siguientes al de la recepción de la solicitud. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, a su vez, la lleve a cabo en su fichero.

3.- La solicitud de rectificación deberá indicar el dato que es erróneo y la corrección que debe realizarse y deberá ir acompañada de la documentación justificativa de la rectificación solicitada, salvo que la misma dependa exclusivamente del consentimiento del interesado.

4.- En la solicitud de cancelación, el interesado deberá indicar si revoca el consentimiento otorgado, en los casos en que la revocación proceda, o si, por el contrario, se trata de un dato erróneo o inexacto, en cuyo caso deberá acompañar la documentación justificativa.

5.- La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos.

6.- Si solicitada la rectificación o cancelación, el responsable del fichero considera que no procede atender la solicitud del afectado, se lo comunicará motivadamente dentro del plazo de los cinco días

siguientes al de la recepción de la misma, a fin de que por éste se pueda hacer uso de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992.

7.- Transcurrido el plazo de cinco días sin que de forma expresa se responda a la solicitud de rectificación o cancelación, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación que corresponda.

8.- La cancelación exige el borrado físico de los datos, sin que sea suficiente a estos efectos una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren las bajas producidas.

9.- En los casos en que, siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, el responsable del fichero procederá al bloqueo de los datos, con el fin de impedir su ulterior proceso o utilización.

Se exceptúa, no obstante, el supuesto en el que se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren.

NORMA CUARTA. FICHEROS DE PRESTACIÓN DE SERVICIOS DE INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y CRÉDITO.

1.- El ejercicio de los derechos de acceso, rectificación y cancelación en el caso de los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito se rige por las normas anteriores de la presente Instrucción, sin perjuicio de lo señalado en los apartados siguientes.

2.- El responsable de un fichero de prestación de servicios de solvencia patrimonial y crédito con datos obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento, estará obligado a satisfacer, en cualquier caso, los derechos de acceso, rectificación y cancelación. Las personas y entidades a las que se presta el servicio únicamente estarán obligadas a comunicar al afectado aquellos datos relativos al mismo a los que ellas tengan acceso y a comunicar la identidad del responsable del fichero común para que pueda completar el ejercicio de sus derechos.

3.- El responsable del fichero común en el que se traten automatizadamente datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés, ante una solicitud de ejercicio del derecho de acceso, deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero. Cualquier otra entidad participante en el sistema, ante tal solicitud, deberá comunicar al afectado todos los datos relativos al mismo a los que ella

pueda acceder, así como la identidad del responsable del fichero común para que pueda completar el ejercicio de su derecho de acceso.

Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige al responsable del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de cinco días, procederá a la rectificación o cancelación cautelar de los mismos.

Si la solicitud del ejercicio de los derechos de rectificación o cancelación de datos se dirige a cualquier otra entidad participante en el sistema y hace referencia a datos que dicha entidad haya facilitado al fichero común, procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al responsable del fichero común en el plazo de cinco días. Si la solicitud hace referencia a datos que la entidad no hubiera facilitado al fichero común, dicha entidad informará al afectado sobre este hecho, proporcionándole, además, la identidad del responsable del fichero común para que pueda completar el ejercicio de sus derechos.

4.- En los ficheros de prestación de servicios de información de solvencia patrimonial y crédito, cualquiera que sea el origen de los datos, cuando el afectado lo solicite el responsable del fichero común deberá cumplir la obligación establecida en el artículo 28.2 de la Ley Orgánica 5/1992 de facilitar , las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios.

NORMA QUINTA. FICHEROS CON FINES DE PUBLICIDAD.

1.- El responsable del fichero que presta el servicio de publicidad estará obligado a satisfacer los derechos de acceso, rectificación y cancelación. La entidad beneficiaria de la publicidad estará obligada a indicar al afectado la identidad del responsable del fichero del que provienen los datos. A tal efecto, se entenderá suficiente que dicha información se haga constar en la campaña publicitaria.

2.- Cuando el interesado manifieste su deseo de no recibir publicidad, y no ejerza expresamente el derecho de cancelación el responsable del fichero podrá conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

DISPOSICIÓN FINAL.- La presente Instrucción entrará en vigor a los 20 días de su publicación en el Boletín Oficial del Estado.

Madrid, 19 de enero de 1998
EL DIRECTOR DE LA AGENCIA,
Fdo.: Juan José Martín-Casallo López

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

EL PARLAMENTO EUROPEO Y EL, CONSEJO DE LA UNIóN EUROPEA,

Visto el Tratado constitutivo de la Comunidad Europea, y, en particular, su artículo 100 A,
Vista la propuesta de la Comisión. [1]
Visto el dictamen del Comité Económico y Social [2]
De conformidad con el procedimiento establecido en el artículo 189 B del Tratado[3],

Considerando que los objetivos de la Comunidad definidos en el Tratado, tal y como quedó modificado por el Tratado de la Unión Europea, consisten en lograr una unión cada vez más estrecha entre los pueblos europeos, establecer relaciones más estrechas entre los Estados miembros de la Comunidad, asegurar, mediante una acción común, el progreso económico y social, eliminando las barreras que dividen Europa, fementar la continua mejora de las condiciones de vida de sus pueblos, preservar y consolidar la paz y la libertad y promover la democracia, basándose en los derechos fundamentales reconocidos en las constituciones Y leyes de los Estados miembros y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales;

Considerando que los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos;

(3) Considerando que el establecimiento Y funcionamiento del mercado interior, dentro del cual está garantizada, con arreglo al artículo 7 A del Tratado, la libre circulación de mercancías, personas, servicios y capitales, hacen necesaria no sólo la libre circulación de datos personales de un Estado miembro a otro, sino también la protección de los derechos fundamentales de las personas;

(4) Considerando que se recurre cada vez más en la Comunidad al tratamiento de datos personales en los diferentes sectores de actividad económica y social; que el avance de las tecnologías de la información facilita considerablemente el tratamiento y el intercambio de dichos datos;

(5) Considerando que la integración económica y social resultante del establecimiento y funcionamiento del mercado interior, definido en el artículo 7 A del Tratado, va a implicar necesariamente un aumento notable de los flujos transfronterizos de datos personales entre todos los agentes de la vida económica y social de los Estados miembros, ya se trate de agentes públicos o privados; que el intercambio de datos personales entre empresas establecidas en los diferentes Estados miembros experimentará un desarrollo; que las administraciones nacionales de los diferentes Estados miembros, en aplicación del Derecho comunitario, están destinadas a colaborar y a intercambiar datos personales a fin de cumplir su cometido o ejercer funciones por cuenta de las administraciones de otros Estados miembros, en el marco del espacio sin fronteras que constituye el mercado interior;

(6) Considerando, por lo demás, que el fortalecimiento de la cooperación científica y técnica, así como el establecimiento coordinado de nuevas redes de telecomunicaciones en la Comunidad exigen y facilitan la circulación transfronteriza de datos personales;

(7) Considerando que las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, estas diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impe*dir* que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario; que estas diferencias en los niveles de protección se deben a la disparidad existente entre las disposiciones legales, reglamentarias y adminis trativas de los Estados miembros;

[1] DO nº C 277 de 5. 11. 1990, p. 3 y DO nº C 311 de 27. 11. 1992, p. 30.
[2] DO nº 159 de 17. 6. 1991, p. 38.
[3] Dictamen del Parlamento Europeo de 11 de marzo de 1992 (DO no C 94 de 13. 4. 1992, p. 198), confirmado el 2 de diciembre de 1993 (DO nº C 342 de 20. 12. 1993, p. 30); posición común del Consejo de 20 de febrero de 1995 (DO nº C 93 de 13. 4. 1995, p. 1) y Decisión del Parlamento Europeo de 15 de junio de 1995 (DO nº C *166 de* 3. 7. 1995).

(8) Considerando que, para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros; que ese objetivo, esencial para el mercado interior, no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el artículo 7 A del Tratado; que, por tanto, es necesario que la Comunidad intervenga para aproximar las legislaciones;

(9) Considerando que, a causa de la protección equivalente que resulta de la aproximación de las legislaciones nacionales, los Estados miembros ya no podrán obstaculizar la libre circulación entre ellos de datos personales por motivos de protección de los derechos y libertades de las personas físicas, y, en particular, del derecho a la intimidad; que los Estados miembros dispondrán de un margen de maniobra del cual podrán servirse, en el contexto de la aplicación de la presente Directiva, los interlocutores económicos y sociales; que los Estados miembros podrán, por lo tanto, precisar en su derecho nacional las condiciones generales de licitud del tratamiento de datos; que, al actuar así, los Estados miembros procurarán mejorar la protección que proporciona su legislación en la actualidad; que, dentro de los límites de dicho margen de maniobra y de conformidad con el Derecho comunitario, podrán surgir disparidades en la aplicación de la presente Directiva, y que ello podrá tener repercusiones en la circulación de datos tanto en el interior de un Estado miembro como en la Comunidad;

(10) Considerando que las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como en los principios generales del Derecho comunitario; que, por lo tanto, la aproximación de dichas legislaciones no debe conducir a una disminución de la protección que garantizan sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la Comunidad;

(11) Considerando que los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, contenidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales;

(12) Considerando que los principios de la protección deben aplicarse a todos los tratamientos de datos personales cuando las actividades del responsable del tratamiento entren en el ámbito de aplicación del Derecho comunitario; que debe excluirse el tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas, como la correspondencia y la llevanza de un repertorio de direcciones;

(13) Considerando que las actividades a que se refieren los títulos V y VI del Tratado de la Unión Europea relativos a la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en el ámbito penal no están comprendidas en el ámbito de aplicación del Derecho comunitario, sin perjuicio de las obligaciones que incumben a los Estados miembros con arreglo al apartado 2 del artículo 56 y a los artículos 57 y 100 A del Tratado; del] tratamiento de los datos de carácter personal que sea necesario para la salvaguardia del bienestar económico del Estado no está comprendido en el ámbito de aplicación de la presente Directiva en los casos en que dicho tratamiento esté relacionado con la seguridad del Estado;

(14) Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos;

(15) Considerando que los tratamientos que afectan a dichos datos sólo quedan amparados por la presente Directiva cuando están automatizados o cuando los datos a que se refieren se encuentran contenidos o se destinan a encontrarse contenidos en un archivo estructurado según criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trata;

(16) Considerando que los tratamientos de datos constituidos por sonido e imagen, como los de la vigilancia por videocámara, no están comprendidos en el ámbito de aplicación de la presente Directiva cuando se aplican con fines de seguridad pública, defensa, seguridad del Estado o para el ejercicio de las actividades del Estado relacionadas con ámbitos del derecho penal o para el ejercicio de otras actividades que no están comprendidos en el ámbito de aplicación del Derecho comunitario;

(17) Considerando que en lo que respecta al tratamiento del sonido y de la imagen aplicados con fines periodísticos o de expresión literaria o artística, en particular en el sector audiovisual, los principios de la Directiva se aplican de forma restringida según lo dispuesto en al artículo 9;

(18) Considerando que, para evitar que una persona sea excluida de la protección garantizada por la presente Directiva, es necesario que todo tratamiento de datos personales efectuado en la Comunidad respete la legislación de uno de sus Estados miembros; que, a este respecto, resulta conveniente someter el tratamiento de datos efectuados por cualquier persona que actúe bajo la autoridad del responsable del tratamiento establecido en un Estado miembro a la aplicación de la legislación de tal Estado;

(19) Considerando que el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto; que cuando un mismo responsable esté establecido en el territorio de varios Estados miembros, en particular por medio de una empresa filial, debe garantizar, en particular para evitar que se eluda la normativa aplicable, que cada uno de los establecimientos cumpla las obligaciones impuestas por el Derecho nacional aplicable a estas actividades;

(20) Considerando que el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deben adaptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva;

(21) Considerando que la presente Directiva no afecta a las normas de territorialidad aplicables en materia penal;

(22) Considerando que los Estados miembros precisarán en su legislación o en la aplicación de las disposiciones adoptadas en virtud de la presente Directiva las condiciones generales de licitud del tratamiento de datos; que, en particular, el artículo 5 en relación con los artículos 7 y 8, ofrece a los Estados miembros la posibilidad de prever, independientemente de las normas generales, condiciones especiales de tratamiento de datos en sectores específicos, así como para las diversas categorías de datos contempladas en el artículo 8;

(23) Considerando que los Estados miembros están facultades para garantizar la protección de las personas tanto mediante una ley general relativa a la protección de las personas respecto del tratamiento, de los datos de carácter personal como mediante leyes sectoriales, como las relativas a los institutos estadísticos;

(24) Considerando que las legislaciones relativas a la protección de las personas jurídicas respecto del tratamiento de los datos que las conciernan no son objeto de la presente Directiva;

(25) Considerando que los principios de la protección tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos- obligaciones relativas, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control v las circunstancias en las que se puede efectuar el 'tratamiento- y, por otra parte, en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento de ser informadas acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias;

(26) Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay

que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; que los códigos de conducta con arreglo al artículo 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado;

(27) Considerando que la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues la contrario daría lugar a riesgos graves de alusión; que, no obstante, por lo que respecta al tratamiento manual, la presente Directiva sólo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas; que, en particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 2, los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva;

(28) Considerando que todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; que debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos; que los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originalmente especificados;

(29) Considerando que el tratamiento ulterior de datos personales, con fines históricos, estadísticos o científicos no debe por lo general considerarse incompatible con los objetivos para los que se recogieron los datos, siempre y cuando los Estados miembros establezcan las garantías adecuadas; que dichas garantías deberán impedir que dichos datos sean utilizados para tomar medidas o decisiones contra cualquier persona;

(30) Considerando que para ser lícito el tratamiento de datos personales debe basarse además en el consentimiento del interesado o ser necesario con vistas a la celebración o ejecución de un contrato que obligue al interesado, o para la observancia de una obligación legal o para el cumplimiento de una misión de interés público o para el ejercicio de la autoridad pública o incluso para la realización de un interés legítimo de una persona, siempre que no prevalezcan los intereses o los derechos y libertades del interesado; que, en particular, para asegurar el equilibrio de los intereses en juego, garantizando a la vez una competencia efectiva, los Estados miembros pueden precisar las condiciones en las que se podrán utilizar y comunicar a terceros datos de carácter personal, en el desempeño de actividades legítimas de gestión ordinaria de empresas y otras entidades; que los Estados miembros pueden asimismo establecer previamente las condiciones en que pueden efectuarse comunicaciones de datos personales a terceros con fines de prospección comercial o de prospección realizada por una institución benéfica u otras asociaciones o fundaciones, por ejemplo de carácter político, dentro del respeto de las disposiciones que permiten a los interesados oponerse, sin alegar los motivos y sin gastos, al tratamiento de los datos que les conciernan;

(31) Considerando que un tratamiento de datos personales debe estimarse lícito cuando se efectúa con el fin de proteger un interés esencial para la vida del interesado;

(32) Considerando que corresponde a las legislaciones nacionales determinar si el responsable del tratamiento que tiene conferida una misión de interés público o inherente al ejercicio del poder público, debe ser una administración pública u otra persona de derecho público o privado, como por ejemplo una asociación profesional;

(33) Considerando, por lo demás, que los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no deben ser objeto de tratamiento alguno, salvo en caso de que el interesado haya dado su consentimiento explícito; que deberán constar de forma

explícita las excepciones a esta prohibición para necesidades específicas, en particular cuando el tratamiento de dichos datos se realice con fines relacionados con la salud, por parte de personas físicas sometidas a una obligación legal de secreto profesional, o para actividades legítimas por parte de ciertas asociaciones o fundaciones cuyo objetivo sea hacer posible el ejercicio de libertades fundamentales;

(34) Considerando que también se deberá autorizar a los Estados miembros, cuando esté justificado por razones de interés público importante, a hacer excepciones a la prohibición de tratar categorías sensibles de datos en sectores como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro enfermedad, la investigación científica y las estadísticas públicas; que a ellos corresponde, no obstante, prever las garantías apropiadas y específicas a los fines de proteger los derechos fundamentales y la vida privada de las personas;

(35) Considerando, además, que el tratamiento de datos personales por parte de las autoridades públicas con fines, establecidos en el Derecho constitucional o en el Derecho internacional público, de asociaciones religiosas reconocidas oficialmente, se realiza por motivos importantes de interés público;

(36) Considerando que, si en el marco de actividades relacionadas con las elecciones, el funcionamiento del sistema democrático en algunos Estados miembros exige que los partidos políticos recaben datos sobre la ideología política de los ciudadanos, podrá autorizarse el tratamiento de estos datos por motivos importantes de interés público, siempre que se establezcan las garantías adecuadas;

(37) Considerando que para el tratamiento de datos personales con fines periodísticos o de expresión artística o literaria, en particular en el sector audiovisual, deben preverse excepciones o restricciones de determinadas disposiciones de la presente Directiva siempre que resulten necesarias para conciliar

los derechos fundamentales de la persona con la libertad de expresión y, en particular, la libertad de recibir o comunicar informaciones, tal y como se garantiza en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales; que por lo tanto, para ponderar estos derechos fundamentales, corresponde a los Estados miembros prever las excepciones y las restricciones necesarias en lo relativo a las medidas generales sobré la legalidad del tratamiento de datos, las medidas sobre la transferencia de datos a terceros países y las competencias de las autoridades de control sin que esto deba inducir, sin embargo, a los Estados miembros a prever excepciones a las medidas que garanticen la seguridad del tratamiento; que, igualmente, debería concederse a la autoridad de control responsable en la materia al menos una serie de competencias *a posteriori* como por ejemplo publicar periódicamente un informe al respecto o bien iniciar procedimientos legales ante las autoridades judiciales;

(38) Considerando que el tratamiento leal de datos supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención;

(39) Considerando que determinados tratamientos se refieren a datos que el responsable no ha recogido directamente del interesado; que, por otra parte, pueden comunicarse legítimamente datos a un tercero aún cuando dicha comunicación no estuviera prevista en el momento de la recogida de los datos del propio interesado; que, en todos estos supuestos**,** debe informarse al interesado en el momento del registro de los datos o, a más tardar, al comunicarse los datos por primera vez a un tercero;

(40) Considerando, no obstante, que no es necesario imponer esta obligación si el interesado ya está informado, si el registro o la comunicación están expresamente previstos por la ley o si resulta imposible informarle, o ello implica esfuerzos desproporcionados, como puede ser el caso para tratamientos con fines históricos, estadísticos o científicos; que a este respecto pueden tomarse en consideración el número de interesados, la antigüedad de los datos, y las posibles medidas compensatorias;

(41) Considerando que cualquier persona debe disfrutar del derecho de acceso a los datos que le conciernan y sean objeto de tratamiento, para cerciorarse, en particular, de su exactitud y de la licitud de su tratamiento; que por las mismas razones cualquier persona debe tener además el derecho de conocer la lógica que subyace al tratamiento automatizado de los datos que la conciernan, al menos en el caso de las decisiones automatizados a que se refiere el apartado 1 del artículo 15; que este derecho no debe menoscabar el secreto de los negocios ni la propiedad intelectual y en particular el derecho de autor que proteja el programa informática; que no obstante esto no debe suponer que se deniegue cualquier información al interesado;

(42) Considerando que, en interés del interesado de que se trate y para proteger los derechos y libertades de terceros, los Estados miembros podrán limitar los derechos de acceso y de información; que podrán, por ejemplo, precisar que el acceso a los datos de carácter médico únicamente pueda obtenerse a través de un profesional de la medicina;

(43) Considerando que los Estados miembros podrán imponer restricciones a los derechos de acceso e información y a determinadas obligaciones del responsable del tratamiento, en la medida en que sean estrictamente necesarias para, por ejemplo, salvaguardar la seguridad del Estado, la defensa, la seguridad pública, los intereses económicos o financieros importantes de un Estado miembro o de la Unión, así como para realizar investigaciones y entablar procedimientos penales y perseguir violaciones de normas deontológicas en las profesiones reguladas; que conviene enumerar, a efectos de excepciones y limitaciones, las tareas de control, inspección o reglamentación necesarias en los tres últimos sectores mencionados relativos a la seguridad pública, los intereses económicos o financieros y la represión penal; que esta enumeración de tareas relativas a los tres sectores citados no afecta a la legitimidad de las excepciones y restricciones establecidas por razones de seguridad del Estado o de defensa;

(44) Considerando que los Estados miembros podrán verse obligados, en virtud de las disposiciones del Derecho comunitario, a establecer excepciones a las disposiciones de la presente Directiva relativas al derecho de acceso, a la información de personas y a la calidad de los datos para garantizar algunas de las finalidades contempladas más arriba;

(45) Considerando que cuando se pudiera efectuar lícitamente un tratamiento de datos por razones de interés público o del ejercicio de la autoridad pública, o en interés legítimo de una persona física, cualquier persona deberá, sin embargo, tener derecho a oponerse a que los datos que le conciernan sean objeto de un tratamiento, en virtud de motivos fundados y legítimos relativos a su situación concreta; que los Estados miembros tienen, no obstante, la posibilidad de establecer disposiciones nacionales contrarias;

(46) Considerando que la protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado; que corresponde a los Estados miembros velar por que los responsables del tratamiento respeten dichas medidas; que esas medidas deberán garantizar un nivel de seguridad adecuado teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse;

(47) Considerando que cuando un mensaje con datos personales sea transmitido a través de un servicio de telecomunicaciones o de correo electrónico cuyo único objetivo sea transmitir mensajes de ese tipo, será considerada normalmente responsable del tratamiento de los datos personales presentes en el mensaje aquella persona de quien proceda el mensaje y no la que ofrezca el servicio de transmisión; que, no obstante, las personas que ofrezcan estos servicios normalmente serán consideradas responsables del tratamiento de los datos personales complementarios y necesarios para el funcionamiento del servicio;

(48) Considerando que los procedimientos de notificación a la autoridad de control tienen por objeto asegurar la publicidad de los fines de los tratamientos y de sus principales características a fin de controlarlos a la luz de las disposiciones nacionales adoptadas en aplicación de la presente Directiva;

(49) Considerando que para evitar trámites administrativos improcedentes, los Estados miembros pueden establecer exenciones o simplificaciones de la notificación para los tratamientos que no atenten contra los derechos y las libertades de los interesados, siempre y cuando sean conformes a un acto adoptado por el Estado miembro en el que se precisen sus límites; que los Estados miembros pueden igualmente disponer la exención o la simplificación cuando un encargado, nombrado por el responsable del tratamiento, se cerciore de que los tratamientos efectuados no pueden atentar contra los derechos Y libertades de los interesados; que la persona encargada de la protección de los datos, sea o no empleado del responsable del tratamiento de datos, deberá ejercer sus funciones con total independencia;

(50) Considerando que podrán establecerse exenciones o simplificaciones para los tratamientos cuya única finalidad sea el mantenimiento de registros destinados, de conformidad con el Derecho nacional, a la información del público y que sean accesibles para la consulta del público o de toda persona que justifique un interés legítimo;

(51) Considerando, no obstante, que el beneficio de la simplificación o de la exención de la obligación de notificación no dispensa al responsable del tratamiento de ninguna de las demás obligaciones derivadas de la presente Directiva;

(52) Considerando que, en este contexto, el control a *posterior¡* por parte de las autoridades competentes debe considerarse, en general, una medida suficiente;

(53) Considerando, no obstante, que determinados tratamientos pueden presentar riesgos particulares desde el punto de vista de los derechos y las libertades de los interesados, ya sea por su naturaleza, su alcance o su finalidad, como los de excluir a los interesados del beneficio de un derecho, de una prestación o de un contrato, 9 por el uso particular de una tecnología nueva; que es competencia de los Estados miembros, si así lo desean, precisar tales riesgos en sus legislaciones;

(54) Considerando que, a la vista de todos los tratamientos llevados a cabo en la sociedad, el número de los que presentan tales riesgos particulares debería ser muy limitado; que los Estados miembros deben prever, para dichos tratamientos, un examen previo a su realización por parte de la autoridad de control o del encargado de la protección de datos en cooperación con aquélla; que, tras dicho control previo, la autoridad de control, en virtud de lo que disponga su Derecho nacional, podrá emitir un dictamen o autorizar el tratamiento de datos; que este examen previo podrá realizarse también en el curso de la elaboración de una medida legislativa aprobada por el Parlamento nacional o de una medida basada en dicha medida legislativa, que defina la naturaleza del tratamiento y precise las garantías adecuadas;

(55) Considerando que las legislaciones nacionales deben prever un recurso judical para los casos en los que el responsable del tratamiento de datos no respete los derechos de los interesados; que los daños que pueden sufrir las personas a raíz de un tratamiento ¡lícito han de ser reparados por el responsable del tratamiento de datos, el cual sólo podrá ser eximido de responsabilidad si demuestra que no le es imputable el hecho perjudicial, principalmente si demuestra la responsabilidad del interesado o un caso de fuerza mayor; que deben imponerse sanciones a toda persona, tanto de derecho privado como de derecho público, que no respete las disposiciones nacionales adoptadas en aplicación de la presente Directiva;

(56) Considerando que los flujos transfronterizos de datos personales son necesarios para la desarrollo del comercio internacional; que la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado; que el carácter adecuado del nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias;

(57) Considerando, por otra parte, que cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales;

(58) Considerando que han de establecerse excepciones a esta prohibición en determinadas circunstancias, cuando el interesado haya dado su consentimiento, cuando la transferencia sea necesaria en relación con un contrato o una acción judicial, cuando así lo exija la protección de un interés público importante, por ejemplo en casos de transferencia internacional de datos entre las administraciones fiscales o aduaneras o entre los servicios competentes en materia de seguridad

social, o cuando la transferencia se haga desde un registro previsto en la legislación con fines de consulta por el público o por personas con un interés legítimo; que en tal caso dicha transferencia no debe afectar a la totalidad de los datos o las categorías de datos que contenga el mencionado registro; que, cuando la finalidad de un registro sea la consulta por parte de personas que tengan un interés legítimo, la transferencia sólo debería poder efectuarse a petición de dichas personas o cuando éstas sean las destinatarias;

(59) Considerando que pueden adaptarse medidas particulares para paliar la insuficiencia del nivel de protección en un tercer país, en caso de que el responsable del tratamiento ofrezca garantías adecuadas; que, por lo demás, deben preverse procedimientos de negociación entre la Comunidad y los países terceros de que se trate;

(60) Considerando que, en cualquier caso, las transferencias hacia países terceros sólo podrán efectuarse si se respetan plenamente las disposiciones adoptadas por los Estados miembros en aplicación de la presente Directiva, Y, en particular, de su artículo 8;

(61) Considerando que los Estados miembros y la Comisión, dentro de sus respectivas competencias, deben alentar a los sectores profesionales para que elaboren códigos de conducta a fin de facilitar, habida cuenta del carácter específico del tratamiento de datos efectuado en determinados sectores, la aplicación de la presente Directiva respetando las disposiciones nacionales adoptadas para su aplicación;

(62) Considerando que la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales;

(63) Considerando que dicha autoridad debe disponer de los medios necesarios para cumplir su función, ya se trate de poderes de investigación o de intervención, en particular en casos de reclamaciones presentadas a la autoridad o de poder comparecer en juicio; que tal autoridad ha de contribuir a la transparencia de los tratamientos de datos efectuados en el Estado miembro del que dependa;

(64) Considerando que las autoridades de los distintos Estados miembros habrán de prestarse ayuda mutua en el ejercicio de sus funciones-, de forma que se garantice el pleno respeto de las normas de protección en toda la Unión Europea;

(65) Considerando que se debe crear, en el ámbito comunitario, un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, el cual habrá de ejercer sus funciones con plena independencia; que, habida cuenta de este carácter específico, el grupo deberá asesorar a la Comisión y contribuir, en particular, a la aplicación uniforme de las normas nacionales adoptadas en aplicación de la presente Directiva;

(66) Considerando que, por lo que respecta a la transferencia de datos hacia países terceros, la aplicación de la presente Directiva requiere que se atribuya a la Comisión competencias de ejecución y que se cree un procedimiento con arreglo a las modalidades establecidas en la Decisión 87/373/CEE del Consejo.[4]

(67) Considerando que el 20 de diciembre de 1994 se alcanzó un acuerdo sobre un *modus vivendi entre* el Parlamento Europeo, el Consejo y la Comisión concerniente a las medidas de aplicación de los actos adoptados de conformidad con el procedimiento establecido en el artículo 189 B del Tratado CE;

(68) Considerando que los principios de protección de los derechos y libertades de las personas v, en particular, del respeto de la intimidad en lo que se refiere al tratamiento de los datos personales objeto de la presente Directiva podrán completarse o precisarse, sobre todo en determinados sectores, mediante normas específicas conformes a estos principios;

(69) Considerando que resulta oportuno conceder a los Estados miembros un plazo que no podrá ser superior a tres años a partir de la entrada en vigor de las medidas nacionales de transposición de la presente Directiva, a fin de que puedan aplicar de manera progresiva las nuevas disposiciones

[4] DO nº L197 de 18.7. 1987, p. 33.

nacionales mencionadas a todos los tratamientos de datos va existentes; que, con el fin de facilitar una aplicación que presente una buena relación coste eficacia, se concederá a los Estados miembros un período suplementario que expirará a los doce años de la fecha en que se adopte la presente Directiva, para garantizar que los ficheros manuales existentes en dicha fecha se hayan ajustado a las disposiciones de la Directiva; que si los datos contenidos en dichos ficheros son tratados efectivamente de forma manual en ese período transitorio ampliado deberán, sin embargo, ser ajustados a dichas disposiciones cuando se realice tal tratamiento;

(70) Considerando que no es procedente que el interesado tenga que dar de nuevo su consentimiento a fin de que el responsable pueda seguir efectuando, tras la entrada en vigor de las disposiciones nacionales adoptadas en virtud de la presente Directiva, el tratamiento de datos sensibles necesario para la ejecución de contratos celebrados previo consentimiento libre e informado antes de la entrada en vigor de las disposiciones mencionadas;

(71) Considerando que la presente Directiva no se opone a que un Estado miembro regule las actividades de prospección comercial destinadas a los consumidores que residan en su territorio, en la medida en que dicha regulación no afecte a la protección de las personas en lo que respecta a tratamientos de datos personales;

(72) Considerando que la presente Directiva autoriza que se tenga en cuenta el principio de acceso público a los documentos oficiales a la hora de aplicar los principios expuestos en la presente Directiva,

HAN ADOPTADO LA PRESENTE DIRECTIVA:

CAPÍTULO 1

DISPOSICIONES GENERALES

Artículo 1

Objeto de la Directiva

1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.

Artículo 2

Definiciones

A efectos de la presente Directiva, 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,, («tratamiento,»: cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta,

utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;

c) “fichero de datos personales” (“fichero”): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

d) «responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos ,personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;

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

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

g) “destinatario”: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios;

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

Artículo 3

Ámbito de aplicación

1. Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

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

- efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal;

- efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

Artículo 4

Derecho nacional aplicable

1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:

a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté

establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;

b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público;

c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.

2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

Capítulo II

Condiciones Generales Para La Licitud Del Tratamiento De Datos Personales

Artículo 5

Los Estados miembros precisarán, dentro de los límites de las disposiciones del presente capítulo, las condiciones en que son lícitos los tratamientos de datos personales.

Sección 1 Principios Relativos A La Calidad De Los Datos

Artículo 6

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

a) tratados de manera leal y lícita;

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

c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;

d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;

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

2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado

Sección II Principios Relativos A La Legitimación Del TraTamiento De Datos

Artículo 7

Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

a) el interesado ha dado su consentimiento de forma inequívoca, o

b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o

c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o

d) es necesario para proteger el interés vital del interesado, o

e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o

f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.

Sección III Categorías Especiales De Tratamientos

Artículo 8 Tratamiento de categorías especiales de datos

1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

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

a) el interesado haya dado su consentimiento explícito a dicho tratamien to, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o

b) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o

c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o

d) el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asocia ción o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, 0

e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

3. El apartado 1 no se aplicará cuando el tratamiento de datos 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 sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las

autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto.

4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control.

5. El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos.

Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos.

6. Las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión.

7. Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento.

Artículo 9

Tratamiento de datos personales y libertad de expresión

En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión.

Sección IV Información Del Interesado

Artículo 10 Información en caso de obtención de datos recabados del propio interesado

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

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

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

c) cualquier otra información tal como:

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

- el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder,

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

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

Artículo 11 Información cuando los datos no han sido recabados del propio interesado

1. Cuando los datos no hayan sido recabados del interesado, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la información que se enumera a continuación, salvo si el interesado ya hubiera sido informado de ello:

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

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

c) cualquier otra información tal como:

- las categorías de los datos de que se trate,

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

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

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

2. Las disposiciones del apartado 1 no se aplicarán, en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas.

Sección V Derecho De Acceso Del Interesado A Los Datos

Artículo 12 Derecho de acceso

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

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

- la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran Y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos;

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

- el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizados a que se refiere el apartado 1 del artículo 15;

b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos;

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

Sección Vi Excepciones Y Limitaciones

Artículo 13 Excepciones y limitaciones

1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones Y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;

e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;

f) tina función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);

g) la protección del interesado o de los derechos y libertades de otras personas.

2. Sin perjuicio de las garantías legales apropiadas, que
excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas.

Sección VII Derecho De Oposición Del Interesado

Artículo 14 Derecho De Oposición Del Interesado

Los Estados miembros reconocerán al interesado el derecho a:

a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;

b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente, el derecho de oponerse, sin gastos, a dicha comunicación o utilización.

Los Estados miembros adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia del derecho a que se refiere el párrafo primero de la letra b).

Artículo 15 Decisiones individuales automatizados

1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente

en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.

2. Los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo;
0

b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

Sección VIII Confidencialidad Y Seguridad Del Tratamiento

Artículo 16. Confidencialidad del tratamiento

Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal.

Artículo 17. Seguridad del tratamiento

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ¡lícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ¡lícito de datos personales.

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. Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.

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

- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;

- que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

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

SECCIóN IX

Notificación

Artículo 18. Obligación de notificación a la autoridad de control

1. Los Estados miembros dispondrán que el responsable del tratamiento o, en su caso, su representante, efectúe una notificación a la autoridad de control contemplada en el artículo 28, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos, total o parcialmente automatizados, destinados a la consecución de un fin o de varios fines conexos.

2. Los Estados miembros podrán disponer la simplificación o la omisión de la notificación, sólo en los siguientes casos y con las siguientes condiciones:

- cuando, para las categorías de tratamientos que no puedan afectar a los derechos y libertades de los interesados habida cuenta de los datos a que se refiere el tratamiento, los Estados miembros precisen los fines de los tratamientos, los datos o categorías de datos tratados, la categoría o categorías de los interesados, los destinatarios o categorías de destinatarios a los que se comuniquen los datos y el período de conservación de los datos y/o

- cuando el responsable del tratamiento designe, con arreglo al Derecho nacional al que está sujeto, un encargado de protección de los datos personales que tenga por cometido, en particular:

- hacer aplicar en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en virtud de la presente Directiva,

- llevar un registro de los tratamientos efectuados por el responsable del tratamiento, que contenga la información enumerada en el apartado 2 del artículo 21,

garantizando así que el tratamiento de los datos no pueda ocasionar una merma de los derechos y libertades de los interesados.

3. Los Estados miembros podrán disponer que no se aplique el apartado 1 a aquellos tratamientos cuya única finalidad sea la de llevar un registro que, en virtud de disposiciones legales o reglamentarias, esté destinado a facilitar información al público y estén abiertos a la consulta por el público en general o por toda persona que pueda demostrar un interés legítimo.

4. Los Estados miembros podrán eximir de la obligación de notificación o disponer una simplificación de la misma respecto de los tratamientos a que se refiere la letra d) del apartado 2 del artículo S.

5. Los Estados miembros podrán disponer que los tratamientos no automatizados de datos de carácter personal o algunos de ellos sean notificados eventualmente de una forma simplificada.

Artículo 19. Contenido de la notificación

1. Los Estados miembros determinarán la información que debe figurar en la notificación, que será como mínimo:

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

b) el o los objetivos del tratamiento;

c) una descripción de la categoría o categorías de interesados y de los datos o categorías de datos a los que se refiere el tratamiento;

d) los destinatarios o categorías de destinatarios a los que se pueden comunicar los datos;

e) las transferencias de datos previstas a países terceros;

f) una descripción general que permita evaluar de modo preliminar si las medidas adoptadas en aplicación del artículo 17 resultan adecuadas para garantizar la seguridad del tratamiento.

2. Los Estados miembros precisarán los procedimientos
por los que se notificarán a la autoridad de control las modificaciones que afecten a la información contemplada en el apartado 1.

Artículo 20. Controles previos

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

2. Estas comprobaciones previas serán realizadas por la autoridad de control una vez que haya recibido la notificación del responsable del tratamiento o por el encargado de la protección de datos quien, en caso de duda, deberá **consultar** a la autoridad de control.

3. Los Estados miembros podrán también llevar a cabo dicha comprobación en el marco de la elaboración de una norma aprobada por el Parlamento o basada en la misma norma, que defina el carácter del tratamiento y establezca las oportunas garantías.

Artículo 21. Publicidad de los tratamientos

1. Los Estados miembros adoptarán las medidas necesarias para garantizar la publicidad de los tratamientos.

2. Los Estados miembros establecerán que la autoridad de control lleve un registro de los tratamientos notificados con arreglo al artículo 18.

En el registro se harán constar, como mínimo, las informaciones a las que se refieren las letras a) a e) del apartado 1 del artículo 19.

El registro podrá ser consultado por cualquier persona.

3. Los Estados miembros dispondrán, en lo que respecta a los tratamientos no sometidos a notificación, que los responsables del tratamiento u otro órgano designado por los Estados miembros comuniquen, en la forma adecuada, a toda persona que lo solicite, al menos las informaciones a que se refieren las letras a) a e) del apartado 1 del artículo 19.

Los Estados miembros podrán establecer que esta disposición no se aplique a los tratamientos cuyo fin único sea llevar un registro, que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo.

Capítulo III Recursos Judiciales, Responsabilidad Y Sanciones

Artículo 22. Recursos

Sin perjuicio del recurso administrativo que pueda interponerse, en particular ante la autoridad de control mencionada en el artículo 28, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate.

Artículo 23. Responsabilidad

1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en

aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido.

2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño.

Artículo 24 Sanciones

Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva.

CAPÍTULO IV

Transferencia De Datos Personales A Países Terceros

Artículo 25. Principios

1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.

2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias 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, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

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

4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estado miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate.

5. La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4.

6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

Artículo 26. Excepciones

1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:

a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o

c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o

d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o

e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o

f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

3. Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2.

En el supuesto de que otro Estado miembro o la Comisión expresaron su oposición y la justificaran debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

4. Cuando la Comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

CAPíTULO V

CóDIGOS DE CONDUCTA

Artículo 27

1. Los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva.

2. Los Estados miembros establecerán que las asociaciones profesionales, y las demás organizaciones representantes de otras categorías de responsables de tratamientos, que hayan elaborado proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar códigos nacionales existentes puedan someterlos a examen de las autoridades nacionales.

Los Estados miembros establecerán que dicha autoridad vele, entre otras cosas, por la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, la autoridad recogerá las observaciones de los interesados o de sus representantes.

3. Los proyectos de códigos comunitarios, así como las modificaciones o prórrogas de códigos comunitarios existentes, podrán ser sometidos a examen del grupo contemplado en el artículo 29. Éste se pronunciará, entre otras cosas, sobre la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, el Grupo recogerá las observaciones de los interesados o de sus representantes. La Comisión podrá efectuar una publicidad adecuada de los códigos que hayan recibido un dictamen favorable del grupo.

CAPíTULO VI

AUTORIDAD DE CONTROL Y GRUPO DE PROTECCIóN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

Artículo 28

Autoridad de control

1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva.

Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.

2. Los Estados miembros dispondrán que se consulte a las autoridades de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal.

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

- 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;

- poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o 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;

- capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva 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.

4. Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, 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.

Toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la presente Directiva. Dicha persona será informada en todos los casos de que ha tenido lugar una verificación.

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

6. Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro

los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro.

Las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen útil.

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

Artículo 29

Grupo de protección de las personas en lo que respecta al tratamiento de datos personales.

1. Se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, en lo sucesivo denominado <Grupo».

Dicho Grupo tendrá carácter consultivo e independiente.

2. El Grupo estará compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión.

Cada miembro del Grupo será designado por la institución, autoridad o autoridades a que represente. Cuando un Estado miembro haya designado varias autoridades de control, éstas nombrarán a un representante común. Lo mismo harán las autoridades creadas por las instituciones y organismos comunitarios.

3. El Grupo tomará sus decisiones por mayoría simple de los representantes de las autoridades de control.

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

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

6. El Grupo aprobará su reglamento interno.

7. El Grupo examinará los asuntos incluidos en el orden del día por su presidente, bien por iniciativa de éste, bien previa solicitud de un representante de las autoridades de control, bien a solicitud de la Comisión.

Artículo 30

1. El Grupo tendrá por cometido:

a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea;

b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros;

c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adaptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades;

d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria.

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

3. El Grupo podrá, por iniciativa propia, formular recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de datos personales en la Comunidad.

4. Los dictámenes y recomendaciones del Grupo se transmitirán a la Comisión Y al Comité contemplado en el artículo 31.

5. La Comisión informará al Grupo del curso que haya dado a los dictámenes y recomendaciones. A tal efecto, elaborará un informe, que será transmitido asimismo al

Parlamento Europeo y al Consejo. Dicho informe será publicado.

6. El Grupo elaborará un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad y en los países terceros, y lo transmitirá al Parlamento Europeo, al Consejo y a la Comisión. Dicho informe será publicado.

CAPíTULO VII

MEDIDAS DE EJECUCIóN COMUNITARIAS

Artículo 31

El Comité

1. La Comisión estará asistida por un Comité compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión.

2. El representante de la Comisión presentará al Comité un proyecto de las medidas que se hayan de adoptar. El Comité emitirá su dictamen sobre dicho proyecto en un plazo que el presidente podrá determinar en función de la urgencia de la cuestión de que se trate.

El dictamen se emitirá según la mayoría prevista en el apartado 2 del artículo 148 del Tratado. Los votos de los representantes de los Estados miembros en el seno del Comité se ponderarán del modo establecido en el artículo anteriormente citado. El presidente no tomará parte en la votación.

La Comisión adoptará las medidas que serán de aplicación inmediata. Sin embargo, si dichas medidas no fueren conformes al dictamen del Comité, habrán de ser comunicadas sin demora por la Comisión al Consejo. En este caso:

- la Comisión aplazará la aplicación de las medidas que ha decidido por un período de tres meses a partir de la fecha de dicha comunicación;

- el Consejo, actuando por mayoría cualificada, podrá adoptar una decisión diferente dentro del plazo de tiempo mencionado en el primer guión.

DISPOSICIONES FINALES

Artículo 32

1. Los Estados miembros adoptarán las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva, a más tardar al final de un período de tres años a partir de su adopción.

Cuando los Estados miembros adopten dichas disposiciones, éstas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros velarán por que todo tratamiento ya iniciado en la fecha de entrada en vigor de las disposiciones de Derecho nacional adoptadas en virtud de la presente Directiva se ajuste a dichas disposiciones dentro de un plazo de tres años a partir de dicha fecha.

No obstante lo dispuesto en el párrafo primero, los Estados miembros podrán establecer que el tratamiento de datos que ya se encuentren incluidos en ficheros manuales en la fecha de entrada en vigor de las disposiciones nacionales adoptadas en aplicación de la presente Directiva, deba ajustarse a lo dispuesto en los artículos 6, 7 y 8 en un plazo de doce años a partir de la adopción de la misma. No obstante, los Estados miembros otorgarán al interesado, previa solicitud y, en particular, en el ejercicio de su derecho de acceso, el derecho a que se rectifiquen, supriman o bloqueen los datos incompletos, inexactos o que hayan sido conservados de forma incompatible con los fines legítimos perseguidos por el responsable del tratamiento.

3. No obstante lo dispuesto en el apartado 2, los Estados miembros podrán disponer, con sujeción a las garantías adecuadas, que los datos conservados únicamente a efectos de investigación histórica no deban ajustarse a lo dispuesto en los artículos 6, 7 y 8 de la presente Directiva.

4. Los Estados miembros comunicarán a la Comisión el texto de las disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

Artículo 33

La Comisión presentará al Consejo y al Parlamento Europeo periódicamente y por primera vez en un plazo de tres años a partir de la fecha mencionada en el apartado 1 del artículo 32 un informe sobre la aplicación de la presente Directiva, acompañado, en su caso, de las oportunas propuestas de modificación. Dicho informe será publicado.

La Comisión estudiará, en particular, la aplicación de la presente Directiva al tratamiento de datos que consistan en sonidos e imágenes relativos a personas físicas y presentará las propuestas pertinentes que puedan resultar necesarias en función de los avances de la tecnología de la información, y a la luz de los trabajos de la sociedad de la información.

Artículo 34

Los destinatarios de la presente Directiva serán los Estados miembros.

Hecho en Luxemburgo, el 24 de octubre de 1995.

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*
K. HANSCH	L. ATIENZA SERNA

DO nº C 277 de 5. 11. 1990, p. 3 y DO nº C 311 de 27. 11. 1992, p. 30.
(2) DO nº 159 de 17. 6. 1991, p. 38.
(3) Dictamen del Parlamento Europeo de 11 de marzo de 1992 (DO no C 94 de 13. 4. 1992, p. 198), confirmado el 2 de diciembre de 1993 (DO nº C 342 de 20. 12. 1993, p. 30); posición común del Consejo de

20 de febrero de 1995 (DO nº C 93 de 13. 4. 1995, p. 1) y Decisión del Parlamento Europeo de 15 de junio de 1995 (DO nº C *166 de* 3. 7. 1995).

REGLAMENTO DE MEDIDAS DE SEGURIDAD DE LOS FICHEROS AUTOMATIZADOS QUE CONTENGAN DATOS DE CARÁCTER PERSONAL

CAPÍTULO I.- DISPOSICIONES GENERALES

Artículo 1.- Ámbito de aplicación y fines.

El presente Reglamento tiene por objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal.

Artículo 2.- Definiciones.

A efectos de este Reglamento, se entenderá por:

1.- **Sistema de información:** Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

2.- **Usuario**: Sujeto o proceso autorizado para acceder a datos o recursos.

3.- **Recurso**: Cualquier parte componente de un sistema de información.

4.- Accesos autorizados: Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

5.- **Identificación**: Procedimiento de reconocimiento de la identidad de un usuario.

6.- **Autenticación**: Procedimiento de comprobación de la identidad de un usuario.

7.- **Control del acceso**: Mecanismo que en función a la identificación ya autenticada permite acceder a datos o recursos.

8.- **Contraseña**: Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

9.- **Incidencia**: Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

10.- **Soporte**: Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

11.- **Responsable de seguridad**: Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

12.- **Copia de respaldo:** Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación**.**

Artículo 3.- Niveles de seguridad.

1.- Las medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto.

2.- Dichos niveles se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

Artículo 4.- Aplicación de los niveles de seguridad.

1.- Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.

2.- Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el articulo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.

3.- Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas como de nivel alto.

4.- Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20.

5.- Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes.

Artículo 5.- Acceso a datos a través de redes de comunicaciones.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Artículo 6.- Régimen de trabajo fuera de los locales de la ubicación del fichero.

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

Artículo 7.- Ficheros temporales.

1.- Los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en el presente Reglamento.

2.- Todo fichero temporal será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II.- MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 8.- Documento de seguridad.

1.- El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

2.- El documento deberá contener, como mínimo, los siguientes aspectos:

a.- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
b.- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
c.- Funciones y obligaciones del personal.
d.- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e.- Procedimiento de notificación, gestión y respuesta ante las incidencias.
f.- Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

3.- El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

4.- El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Artículo 9.- Funciones y obligaciones del personal.

1.- Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas, de acuerdo con lo previsto en el artículo 8.2.c)

2.- El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 10.- Registro de incidencias.

El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

Artículo 11.- Identificación y autenticación.

1.- El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan **acceso autorizado** al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.

2.- Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

3.- Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible.

Artículo 12.- Control de acceso.

1.- Los usuarios tendrán **acceso autorizado** únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

2.- El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

3.- La relación de usuarios a la que se refiere el artículo 11.1 de este Reglamento contendrá **el acceso autorizado** para cada uno de ellos.

4.- Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular **el acceso autorizado** sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.

Artículo 13.- Gestión de soportes.

1.- Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

2.- La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada, por el responsable del fichero.

Artículo 14. - Copias de respaldo y recuperación.

1.- El responsable de fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

2.- Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

3.- Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos.

CAPÍTULO III.- MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 15.- Documento de seguridad.

El documento de seguridad deberá contener, además de lo dispuesto en el artículo 8 del presente Reglamento, la identificación del **responsable o responsables** de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

Artículo 16.- Responsable de seguridad.

El responsable del fichero designará **uno o varios responsables de seguridad encargados** de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con este Reglamento.

Artículo 17.- Auditoría.

1.- Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

2.- El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

3.- Los informes de auditoría serán analizados por el responsable de seguridad **competente,** que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

Artículo 18.- Identificación y autenticación.

1. El responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

2. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 19.- Control de acceso físico.

Exclusivamente el personal autorizado en el documento **de seguridad** podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

Artículo 20.- Gestión de soportes.

1.- Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2.- Igualmente, se dispondrá de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

3.- Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

4.- Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

Artículo 21.- Registro de incidencias.

1.- En el registro regulado en el artículo 10 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y , en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2.- Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Artículo 22.- Pruebas con datos reales.

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

CAPÍTULO IV.- MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Artículo 23.- Distribución de soportes.

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

Artículo 24.- Registro de accesos.

1.- De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2.- En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3.- Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable de seguridad sin que se deba permitir, en ningún caso, la desactivación de los mismos.

4.- El período mínimo de conservación de los datos registrados será de dos años.

5.- El responsable de seguridad **competente** se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

Artículo 25.- Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en este Reglamento.

Artículo 26.- Telecomunicaciones.

La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

CAPÍTULO V.- INFRACCIONES Y SANCIONES.

Artículo 27.- Infracciones y sanciones.

1.- El incumplimiento de las medidas de seguridad descritas en el presente Reglamento será sancionado de acuerdo con lo establecido en los artículos 43 y 44 de la Ley Orgánica 5/1992, cuando se trate de ficheros de titularidad privada.

El procedimiento a seguir para la imposición de la sanción a la que se refiere el párrafo anterior será el establecido en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

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 45 de la Ley Orgánica 5/1992.

Artículo 28.- Responsables.

Los responsables de los ficheros, sujetos al régimen sancionador de la Ley Orgánica 5/1992, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal en los términos establecidos en el presente Reglamento.

CAPÍTULO VI.- COMPETENCIAS DEL DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS

Artículo 29.- Competencias del Director de la Agencia de Protección de Datos.

El Director de la Agencia de Protección de Datos podrá, de conformidad con lo establecido en el artículo 36 de la Ley Orgánica 5/1992:

1.- Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica 5/1992.

2.- Ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros cuando no se cumplan las medidas de seguridad previstas en el presente Reglamento.

Disposición transitoria única.- Plazos de implantación de las medidas.

En el caso de sistemas de información que se encuentren en funcionamiento a la entrada en vigor del presente Reglamento, las medidas de seguridad de nivel básico previstas en el presente Reglamento deberán implantarse en el plazo de seis meses desde su entrada en vigor, **las de nivel medio en el plazo de un año y las de nivel alto en el plazo de dos años.**

Cuando los sistemas de información que se encuentren en funcionamiento no permitan tecnológicamente la implantación de alguna de las medidas de seguridad previstas en el presente Reglamento, la adecuación de dichos sistemas y la implantación de las medidas de seguridad deberán realizarse en el plazo máximo de tres años a contar desde la entrada en vigor del presente Reglamento.

REAL DECRETO 195/2000, de 11 de febrero, por el que se establece el plazo para ímplantar las medídas de segurídad de los ficheros automatízados prevístas por el Reglamento aprobado por el Real Decreto 994/1999, de 11 de junío.

El Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio, estableció en su disposición transitoria única los plazos de implantación de las medidas de seguridad para los sistemas de información que se encontraran en funcionamiento en el momento de entrada en vigor de dicho Reglamento.

El «efecto 2000» ha obligado a los responsables de los sistemas informáticos a realizar un considerable esfuerzo de adaptación de dichos sistemas, lo que ha supuesto una dificultad objetiva para poder implantar en el plazo provisto las medidas de seguridad de nivel básico exigidas por el Reglamento. Resulta necesario por todo ello establecer un nuevo plazo para la implantación de estas medidas.

En su virtud, a propuesta de la Ministra de Justicia, previo informe de la Agencia de Protección de Datos, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 11 de febrero de 2000,

D 1 S P 0 N G 0

Artículo único.

Los sistemas de información que se encontraran en funcionamiento a la entrada en vigor del Reglamento, aprobado por el Real Decreto 994/1999, de 11 de junio, deberán implantar las medidas de seguridad de nivel básico previstas por dicho Reglamento en un plazo que finalizará el día 26 de marzo de 2000.

Disposición adicional única.

Con efecto retroactivo, se considerará rehabilitado como plazo para la implantación de las medidas de seguridad de nivel básico, con la consiguiente exención de responsabilidad, el comprendido entre el momento de entrada en vigor del presente Real Decreto y el de conclusión del plazo fijado por el Reglamento aprobado por el Real Decreto 99411999, de 11 de junio.

Disposición final única.

El presente Real Decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado». Dado en Madrid a 11 de febrero de 2000.

JUAN CARLOS R.

La Ministra de Justicia, MARGARITA MARISCALIDE GANTEY MIRóN