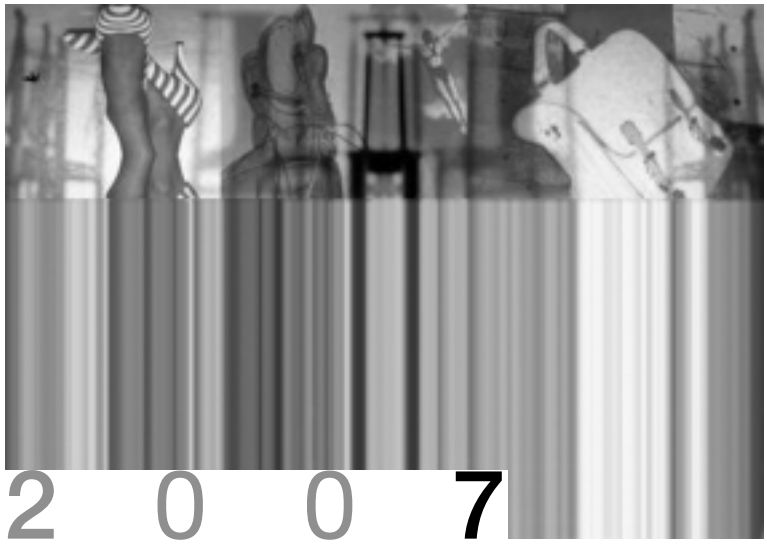
normativa**b**ásica



2 0 0 7

Datuak Babesteko
Euskal Bulegoa

Agencia Vasca de
Protección de Datos

Edición:

Tirada: 600 ejemplares

Edita: Agencia Vasca de Protección de Datos

Internet: www.avpd.es

Impresión: mccgraphics Planta Evagraf

D.L.: VI-000/07

1. LEGISLACIÓN COMUNITARIA

1.1 Directiva 95/46/CE, del Parlamento 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

(DOL núm. 281, de 23 de noviembre de 1995)

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
Visto el dictamen del Comité Económico y Social,
De conformidad con el procedimiento establecido en el artículo 189 B del Tratado

(1) 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, fomentar 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;
(2) 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 impedir 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 administrativas de los Estados miembros;
(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; que el 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 adoptarse 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 facultados 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 y 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 elusión; 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 utili-

zados 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 sobre 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 automatizadas 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 informático; 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 medi-

da 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 posteriori 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, o 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 debe- ría 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 judicial 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 ilícito 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 adoptarse 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;
(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 y, 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 nacionales mencionadas a todos los tratamientos de datos ya 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 I
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 I
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 1.

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 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 tratamiento, 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 asociación 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, o
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 automatizadas 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) una 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 automatizadas.—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; o
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 ilícita, 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 ilícito 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 8.

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 expresaren su oposición y la justificaren 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 adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos persona-

les, 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 comprobare 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.

DISPOSICIONEALES

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.

1.2 Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01). Artículo 8

(DOCEC de 18 de diciembre de 2000 - fragmento)

CAPITULO II
LIBERTADES

Artículo 8.
Protección de datos de carácter personal.—1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

2. CONSTITUCIÓN

2.1 Constitución Española de 27 de diciembre de 1978. Artículo 18

(BOE de 29 de diciembre de 1978 - fragmento)

Artículo 18.
1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

3. LEGISLACIÓN ESTATAL

3.1 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

(BOE núm. 298, de 14 de diciembre de 1999)

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 cance-

lación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.
f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.
j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

TÍTULO II
Principios de la protección de datos

Artículo 4. Calidad de los datos.—1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

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

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

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos 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 prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 5. Derecho de información en la recogida de datos.—1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:
a) De la existencia de un fichero o tratamiento dé datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

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

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

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presenta 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 de 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 art. 16 de la CE, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

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

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

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

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

6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.
También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 8. Datos relativos a la salud.—Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Artículo 9. Seguridad de los datos.—1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

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

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

Artículo 10. Deber de secreto.—El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto

de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11. Comunicación de datos.—1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:
a) Cuando la cesión está autorizada en una ley.
b) Cuando se trate de datos recogidos de fuentes accesibles al público.
c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

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

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

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

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

Artículo 12. Acceso a los datos por cuenta de terceros.—1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

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

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

TÍTULO III
Derechos de las personas

Artículo 13. Impugnación de valoraciones.—1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un trata- miento de datos destinados a evaluar determinados aspectos de su personalidad. 2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad. 3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto. 4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 14. Derecho de consulta al Registro General de Protección de Datos.—Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Artículo 15. Derecho de acceso.—1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

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

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

Artículo 16. Derecho de rectificación y cancelación.—1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán 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 contra prestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

Artículo 18. Tutela de los derechos.—1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

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

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

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

Artículo 19. Derecho a indemnización.—1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

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

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

TÍTULO IV
Disposiciones sectoriales

CAPÍTULO I
FICHEROS DE TITULARIDAD PÚBLICA

Artículo 20. Creación, modificación o supresión.—1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:
a) La finalidad del fichero y los usos previstos para el mismo.
b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
c) El procedimiento de recogida de los datos de carácter personal.
d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
e) Las cesiones de datos de carácter personal y, en su caso, las transferencias dé 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 destinó 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 está 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 CA 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 afecta-

do 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.

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

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

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

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

Artículo 30. Tratamientos con fines de publicidad y de prospección comercial.— 1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

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

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

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

Artículo 31. Censo promocional.—1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.

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

3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estas procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado.

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

Artículo 32. Códigos tipo.—1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.

2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.
En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

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

TÍTULO V
Movimiento internacional de datos

Artículo 33. Norma general.—1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

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

Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. Excepciones.—Lo dispuesto en el artículo anterior no será de aplicación:
a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, 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 aquellas propuestas que éste le realice en el ejercicio de sus funciones.

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

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

Artículo 37. Funciones.—1. 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.

2. Las resoluciones de la Agencia Española de Protección de Datos se harán públicas, una vez hayan sido notificadas a los interesados. La publicación se realizará preferentemente a través de medios informáticos o telemáticos.
Reglamentariamente podrán establecerse los términos en que se lleve a cabo la publicidad de las citadas resoluciones.

Lo establecido en los párrafos anteriores no será aplicable a las resoluciones referentes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos ni a aquéllas por las que se resuelva la inscripción en el mismo de los Códigos tipo, regulados por el artículo 32 de esta ley orgánica.

Artículo 38. Consejo Consultivo.—El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:
Un Diputado, propuesto por el Congreso de los Diputados.
Un Senador, propuesto por el Senado.
Un representante de la Administración Central, designado por el Gobierno.
Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.
Un miembro de la Real Academia de la Historia, propuesto por la misma.
Un experto en la materia, propuesto por el Consejo Superior de Universidades.
Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.
Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.
Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.
El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 39. El Registro General de Protección de Datos.—1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos:
a) Los ficheros de que sean titulares las Administraciones públicas.
b) Los ficheros de titularidad privada.
c) Las autorizaciones a que se refiere la presente Ley.
d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.
e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

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

Artículo 40. Potestad de inspección.—1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.
A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.
Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 41. Órganos correspondientes de las Comunidades Autónomas.— 1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades

de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido.

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

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

Artículo 42. Ficheros de las Comunidades Autónomas en materia de su exclusiva competencia.—1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento.

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

TÍTULO VII
Infracciones y sanciones

Artículo 43. Responsables.—1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.

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

Artículo 44. Tipos de infracciones.—1. Las infracciones se calificarán como leves, graves o muy graves.

2. Son infracciones leves:
a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.
b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.
c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.
d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.
e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

3. Son infracciones graves:
a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.
b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.
c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.
e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada
f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.
g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.
h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.
i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.
j) La obstrucción al ejercicio de la función inspectora.
k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.
l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

4. Son infracciones muy graves:
a) La recogida de datos en forma engañosa y fraudulenta.
b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.
d) No cesar en el uso legítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.
e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.
f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.
h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Artículo 45. Tipo de sanciones.—1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas (601,01 a 60.101,21euros).

2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas (60.101,21 a 300.506,05 euros).

3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas (300.506,05 a 601.012,10 euros).

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

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

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

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

Artículo 46. Infracciones de las Administraciones públicas.—1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las Administraciones públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

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

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

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

Artículo 47. Prescripción.—1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

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

3. Interrumpirá la prescripción la iniciación, con conocimiento de 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.

3. Los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos, en ejercicio de las potestades que a la misma atribuyan esta u otras Leyes, salvo los referidos a infracciones de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, tendrán una duración máxima de seis meses.

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 lícita 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

Disposición adicional primera. *Ficheros preexistentes.*—Los ficheros y tratamientos automatizados inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.
En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica, y la obligación prevista en el párrafo anterior deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995. sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

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

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

Disposición adicional tercera. *Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social.*—Los expedientes específicamente instruidos al amparo, de las derogadas Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social, que contengan datos de cualquier índole susceptibles de afectar a la seguridad, al honor, a la intimidad o a la imagen de las personas, no podrán ser consultados sin que medie consentimiento expreso de los afectados, o hayan transcurrido cincuenta años desde la fecha de aquéllos.
En esté último supuesto, la Administración General del Estado, salvo que haya constancia expresa del fallecimiento de los afectados, pondrá a disposición del solicitante la documentación, suprimiendo de la misma los datos aludidos en el párrafo anterior, mediante la utilización de los procedimientos técnicos pertinentes en cada caso.

Disposición adicional cuarta. *Modificación del art. 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 esta-

blece el apartado 1 del artículo 21 de la Ley Orgánica de Protección de Datos de carácter personal.»

Disposición adicional quinta. *Competencias del Defensor del Pueblo y órganos autonómicos semejantes.*—Lo dispuesto en la presente Ley Orgánica se entiende sin perjuicio de las competencias del Defensor del Pueblo y de los órganos análogos de las Comunidades Autónomas.

Disposición adicional sexta. *Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados.*—Se modifica el artículo 24.3, párrafo 2.0 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

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

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

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

DISPOSICIÓN DEROGATORIA ÚNICA.

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

DISPOSICIONES FINALES

Disposición final primera. *Habilitación para el desarrollo reglamentario.* —El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley.

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

Disposición final tercera. *Entrada en vigor.*—La presente Ley entrará en vigor en el plazo de un mes, contado desde su publicación en el «Boletín Oficial del Estado».
Por tanto, Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta ley Orgánica

3.2 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.

(BOE núm. 147, de 21 de junio de 1994)

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:

CAPITULO 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.

CAPITULO 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.

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

Artículo 7. Inscripción de los ficheros.
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.
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.
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. La inscripción será notificada al responsable del fichero por el Registro General de Protección de Datos.

Artículo 8. Modificación y cancelación de la inscripción.
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.
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.
Los códigos tipo se depositarán, para su inscripción, en el Registro General de Protección de Datos.
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.
Los particulares podrán obtener copias de los códigos tipo depositados e inscritos en el Registro General de Protección de Datos.
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.

CAPITULO 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 trascripción 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. Derecho de rectificación o cancelación.
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.

CAPITULO 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.

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”.

3.3 Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

(BOE núm. 151, de 25 de junio de 1999

El art. 18.4 de la Constitución Española establece que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal, prevé en su art. 9, la obligación del responsable del fichero de adoptar las medidas de índole técnica y organizativas 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 estén expuestos, ya provengan de la acción humana o del medio físico o natural, estableciéndose en el art. 43.3.h) que 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 constituye infracción grave en los términos previstos en la propia Ley.

Sin embargo, la falta de desarrollo reglamentario ha impedido disponer de un marco de referencia para que los responsables promovieran las adecuadas medidas de seguridad y, en consecuencia, ha determinado la imposibilidad de hacer cumplir uno de los más importantes principios de la Ley Orgánica.

El presente Reglamento tiene por objeto el desarrollo de lo dispuesto en los arts. 9 y 43.3.h) de la Ley Orgánica 5/1992. El Reglamento determina las medidas de índole técnica y organizativa que garanticen la confidencialidad e integridad de la información con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado.

Las medidas de seguridad que se establecen se configuran como las básicas de seguridad que han de cumplir todos los ficheros que contengan datos de carácter personal, sin perjuicio de establecer medidas especiales para aquellos ficheros que por la especial naturaleza de los datos que contienen o por las propias características de los mismos exigen un grado de protección mayor.

En su virtud, a propuesta de la Ministra de Justicia, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 11 de junio de 1999,

DISPONGO:

Artículo único. Aprobación del Reglamento

Se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, cuyo texto se inserta a continuación.

Disposición final única. Entrada en vigor

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

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

CAPITULO PRIMERO
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. Sistemas 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 de acceso: mecanismo que en función de 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 del 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 art. 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 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 arts. 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.

CAPITULO II

MEDIDAS DE SEGURIDAD DE NIVEL BASICO

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 art. 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 art. 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 deberá 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 período no se hubiera producido ninguna actualización de los datos.

CAPITULO III

MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 15. Documento de seguridad

El documento de seguridad deberá contener, además de lo dispuesto en el art. 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 art. 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.

CAPITULO 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 competente 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.

CAPITULO 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 arts. 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 art. 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.

CAPITULO 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 art. 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.

DISPOSICION TRANSITORIA

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.

4. NORMATIVA AUTONÓMICA

4.1 Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección De Datos

(BOPV núm. 44, de 4 de marzo de 2004)

EXPOSICIÓN DE MOTIVOS

Los avances de la técnica se han acelerado en los últimos tiempos. Actualmente, el uso de la informática permite tratar gran cantidad de datos relativos a las personas físicas, pudiendo llegar a conocer aspectos relacionados con las mismas que suponen una intromisión en su intimidad. Los ordenamientos jurídicos no pueden permanecer insensibles ante la eventualidad de usos perversos de las posibilidades tecnológicas, en detrimento de espacios que deben quedar reservados a la intimidad personal.

Esta tensión entre tecnología, especialmente en el campo de la informática, e intimidad de las personas apela a una actuación legislativa que procure un equilibrio satisfactorio entre dos bienes dignos de protección jurídica. Por un lado, no es bueno para la sociedad poner freno al desarrollo tecnológico, cuyas potencialidades son inmensas y deben contribuir a un mayor bienestar de la comunidad; pero, por otro, los ciudadanos tienen derecho a que se les proteja su intimidad personal, evitando que las posibilidades que ofrece la tecnología informática actual reduzcan aquélla más allá de lo deseable. Para ello es preciso limitar el uso de la informática y, de este modo, garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Es éste un mandato que el artículo 18.4 de la Constitución impone al legislador, y que éste recoge en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

La preocupación por la protección de la intimidad personal y familiar de los ciudadanos, con la consiguiente limitación del uso de la informática a tal fin, no es exclusiva del legislador estatal. También las instituciones de la Unión Europea han mostrado su sensibilidad en este sentido.

El Tratado de Ámsterdam de 17 de junio de 1997 ha incorporado al tratado constitutivo de la Comunidad Europea su actual artículo 286, que requiere que se apliquen a las instituciones y organismos comunitarios los actos comunitarios relativos a la protección de las personas respecto al tratamiento de datos personales y a la libre circulación de estos datos.

Ya anteriormente, el Parlamento Europeo y el Consejo habían adoptado la Directiva 95/46/CE, 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, donde se recoge el principio de que los sistemas de tratamiento de datos están al servicio del hombre y que deben respetar las libertades y derechos fundamentales de las personas físicas, en particular la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios y al bienestar de los individuos.

Según esta directiva, las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los citados derechos y libertades, particularmente el 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, y considera que la aproximación de dichas legislaciones debe tener por objeto asegurar un alto nivel de protección.

Para la citada directiva, un elemento esencial de la protección de las personas, en lo que respecta a la protección de los datos personales, es la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros, la cual debe dis-

poner de los medios necesarios para cumplir su función, ya se trate de poderes de investigación o de intervención.

La directiva da a los estados miembros un plazo de tres años para la adopción de las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la misma.

La actuación de las instituciones comunitarias en materia de protección de datos no se ha limitado a las directivas destinadas a los estados miembros, sino que también han adoptado medidas destinadas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios, mediante el Reglamento (CE) Nº 45/2001, del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, el cual incluso instituye una autoridad de control independiente (el Supervisor Europeo de Protección de Datos).

Podría decirse que la garantía de un elevado nivel de protección de los datos personales y de la intimidad es un principio inspirador de la normativa comunitaria, que tiene su proyección incluso en propuestas de directiva cuya finalidad no es propiamente la regulación de la protección de los datos de carácter personal, como es el caso de la propuesta de directiva del Parlamento Europeo y del Consejo relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Diario Oficial nº C 365 E de 19/12/2000).

En el Derecho interno, la protección de datos de carácter personal se halla regulada, como decíamos antes, en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que, además de otras materias vinculadas con el derecho fundamental al que se refiere el artículo 18.4 de la Constitución, regula los aspectos básicos del régimen jurídico de la Agencia de Protección de Datos, que es la que se configura como la autoridad de control independiente a la que se refiere la Directiva 95/46/CE.

La ley orgánica establece que la mayor parte de las funciones asignadas a la citada agencia, 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, serán ejercidas 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. Criterio legal que es acorde con el artículo 28 de la Directiva 95/46/CE, según el cual los estados miembros dispondrán de una o más autoridades públicas que se encargarán de vigilar la aplicación, en su territorio, de las disposiciones adoptadas por ellos de acuerdo con la citada directiva, y añade que dichas autoridades ejercerán las funciones que les son atribuidas con total independencia.

Desde el punto de vista de su ordenación sistemática, la ley se halla dividida en tres títulos.

En el título I, de disposiciones generales, se concretan el objeto y el ámbito de aplicación de la ley, delimitando los ficheros que quedan bajo su regulación atendiendo a la Administración pública, institución o corporación que los crea o gestiona. La citada delimitación se completa con la enumeración de los ficheros a los que no se aplicará la ley y de aquellos en los que ésta será de aplicación limitada, por tener regímenes específicos. Contiene también una lista de definiciones muy útil para precisar y unificar la terminología específica de la materia objeto de regulación; se regulan aspectos relacionados con la creación, modificación y supresión de ficheros, limitaciones a la recogida de datos de carácter personal, información a los interesados y seguridad de los ficheros de datos, así como el procedimiento de reclamación ante la Agencia Vasca de Protección de Datos. Se trata de un título necesario para dar coherencia sistemática e integridad a la ley, que requerirá de un desarrollo posterior.

En el título II se crea la Agencia Vasca de Protección de Datos y se regulan los aspectos fundamentales de su régimen jurídico. Contiene preceptos relativos al régimen del personal a su servicio, recursos económicos, régimen presupuestario, órganos de gobierno, funciones y potestades. Es de resaltar la creación del Registro de Protección de Datos como órgano necesario de la agencia.

El título III está dedicado al régimen sancionador. En él se delimitan los sujetos responsables, se tipifican las infracciones y se establecen las sanciones correspondientes. Como dice el

Reglamento (CE) Nº 45/2001, antes citado, un sistema de protección de datos personales requiere establecer derechos y obligaciones, pero también sanciones apropiadas para los infractores. En nuestro caso, dadas las características especiales de los titulares de los ficheros, se presta especial atención al supuesto de infracciones cometidas por el personal al servicio de las administraciones, instituciones y corporaciones a cuyos ficheros se aplica la ley.

La ley contiene tres disposiciones adicionales, relativas a la necesaria comunicación de los ficheros existentes a la Agencia Vasca de Protección de Datos, a la utilización de los datos del padrón municipal por las administraciones autonómica y forales para el ejercicio de sus competencias, y al necesario respeto de las competencias del Ararteko y de la Agencia de Protección de Datos del Estado.

Concluye con una disposición final, en la que se autoriza al Gobierno Vasco para su desarrollo y aplicación.

TÍTULO I.
DISPOSICIONES GENERALES

Artículo 1.- Objeto - La presente ley tiene por objeto: 1. La regulación de los ficheros de datos de carácter personal creados o gestionados por la Comunidad Autónoma del País Vasco, los órganos forales de los territorios históricos y las administraciones locales de la Comunidad Autónoma del País Vasco.

2.- La creación y regulación de la Agencia Vasca de Protección de Datos.

Artículo 2.- Ámbito de aplicación - 1. La presente ley será aplicable a los ficheros de datos de carácter personal creados o gestionados, para el ejercicio de potestades de derecho público, por:

a) La Administración General de la Comunidad Autónoma, los órganos forales de los territorios históricos y las administraciones locales del ámbito territorial de la Comunidad Autónoma del País Vasco, así como los entes públicos de cualquier tipo, dependientes o vinculados a las respectivas administraciones públicas, en tanto que los mismos hayan sido creados para el ejercicio de potestades de derecho público.
b) El Parlamento Vasco.
c) El Tribunal Vasco de Cuentas Públicas.
d) El Ararteko.
e) El Consejo de Relaciones Laborales.
f) El Consejo Económico y Social.
g) El Consejo Superior de Cooperativas.
h) La Agencia Vasca de Protección de Datos.
i) La Comisión Arbitral.
j) Las corporaciones de derecho público, representativas de intereses económicos y profesionales, de la Comunidad Autónoma del País Vasco.
k) Cualesquiera otros organismos o instituciones, con o sin personalidad jurídica, creados por ley del Parlamento Vasco, salvo que ésta disponga lo contrario.

2.- No obstante lo dispuesto en el número anterior, esta ley no será de aplicación a los ficheros:
a) Sometidos a la normativa sobre protección de materias clasificadas.
b) Establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.
c) Regulados por la legislación de régimen electoral.
d) Procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por los cuerpos de Policía del País Vasco, de conformidad con la legislación sobre la materia.

3.- Se regirán por sus disposiciones específicas y, en su caso, por lo especialmente previsto en esta ley los tratamientos de datos personales que sirvan a fines exclusivamente estadísticos y estén amparados por la legislación sobre la función estadística pública.

4.- Las instituciones y centros sanitarios de carácter público y los profesionales a su servicio podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las per-

sonas que a ellos acudan o hayan de ser tratadas en los mismos, de acuerdo con lo dispuesto en la legislación sectorial sobre sanidad, sin perjuicio de la aplicación de lo dispuesto en esta ley en todo lo que no sea incompatible con aquella legislación.

5.- La aplicación de lo dispuesto en esta ley a los ficheros de datos de carácter personal, distintos de los citados en el número 2 de este artículo, creados o gestionados por los cuerpos de Policía del País Vasco se efectuará sin perjuicio de las especificidades de su régimen jurídico previstas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en la Ley 4/1992, de 17 de julio, de Policía del País Vasco.

Artículo 3.- Definiciones - A los efectos de esta ley se entenderá por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables. 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) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuera 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, institución, entidad, corporación u órgano administrativo al que está adscrito el fichero y que decide sobre la finalidad, contenido y uso del tratamiento. La disposición por la que se cree el fichero determinará el responsable del mismo. Sus funciones serán las establecidas en el documento de seguridad.
e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere la letra c) de este artículo.
f) Encargado del tratamiento: 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.
g) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que la conciernen.
h) Cesión o comunicación de datos: toda revelación de datos realizada a persona distinta del interesado.

Artículo 4.- Creación, modificación y supresión de ficheros - 1. La creación, modificación y supresión de ficheros de la Administración de la Comunidad Autónoma se realizará por orden del titular del departamento al que esté adscrito el fichero, la cual deberá contener todas las menciones exigidas por la legislación en vigor y será objeto de publicación en el Boletín Oficial del País Vasco. El procedimiento de elaboración de la citada orden será el previsto para la elaboración de disposiciones de carácter general.

2. En el caso de ficheros de datos de carácter personal de otras administraciones, instituciones o corporaciones, el acuerdo o disposición por la que se cree, modifique o suprima deberá contener todas las menciones exigidas y será publicada en el Boletín Oficial del País Vasco o del territorio histórico, según sea el ámbito territorial al que se extienden sus funciones o competencias.

Artículo 5.- Recogida de datos de carácter personal - Las administraciones públicas y demás instituciones, corporaciones y entidades a que se refiere el artículo 2.1 de esta ley sólo podrán recoger datos de carácter personal para su tratamiento cuando sean adecuados, pertinentes y no excesivos para el ejercicio de las respectivas competencias que tienen atribuidas. Salvo precepto legal en sentido contrario, para la obtención de dichos datos no será preciso recabar el consentimiento de los afectados, pero sólo podrán utilizarse para las finalidades determinadas, explícitas y legítimas para las que se hubieran obtenido, sin perjuicio de su posible tratamiento posterior para fines históricos, estadísticos o científicos, de acuerdo con la legislación aplicable.

Artículo 6.- Información a los interesados - Los interesados a los que se soliciten datos de carácter personal serán previamente informados, de conformidad con la legislación sobre protección de dichos datos. No obstante, cuando los datos no hayan sido recabados del propio interesado y la información a éste resulte imposible o exija esfuerzos desproporcionados, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias, el director de la Agencia Vasca de Protección de Datos, de acuerdo con la susodicha legislación, podrá dispensar al responsable del fichero de la obligación de informar a los interesados.

Artículo 7.- Aprobación del contenido mínimo del documento de seguridad - 1.- l ejercicio de sus potestades de autoorganización, los órganos de gobierno de las administraciones públicas, instituciones y corporaciones a que se refiere el artículo 2.1 de esta ley podrán aprobar, en aplicación de los preceptos relativos a la seguridad de los datos y para aplicar a todos o parte de los ficheros de los que son titulares sus respectivas administraciones, instituciones o corporaciones, el contenido mínimo del documento de seguridad que, en todo caso, deberán elaborar e implantar los responsables de fichero para garantizar la seguridad de los datos de carácter personal contenidos en los citados ficheros.

Artículo 8.- Procedimiento para el ejercicio de los derechos de los interesados - 1.- os interesados podrán ejercitar los derechos de oposición, acceso, rectificación, cancelación y cualesquiera otros que les reconozca la ley. El contenido material de los mismos será el determinado en la ley.

2.- Cada administración, institución o corporación regulará reglamentariamente el procedimiento para el ejercicio de los derechos señalados en el número anterior, en relación con los ficheros de su titularidad a los que es de aplicación esta ley. No se exigirá contraprestación alguna por ello.

Artículo 9.- Reclamaciones ante la Agencia Vasca de Protección de Datos - 1.- as actuaciones contrarias a lo dispuesto en esta ley pueden ser objeto de reclamación por los interesados ante la Agencia Vasca de Protección de Datos, en la forma que reglamentariamente se determine.

2.- El interesado al que se deniegue, total o parcialmente, el ejercicio del derecho de oposición, acceso, rectificación, cancelación o cualquier otro que le reconozca la legislación sobre protección de datos de carácter personal, podrá ponerlo en conocimiento de la Agencia Vasca de Protección de Datos, que deberá asegurarse de la procedencia o improcedencia de la denegación.

3.- El plazo máximo en que se debe dictar y notificar la resolución expresa de tutela de derechos es de seis meses, entendiéndose el silencio administrativo como desestimatorio de la tutela pedida.

4.- Contra las resoluciones de la Agencia Vasca de Protección de Datos procederá recurso contencioso-administrativo. Podrá interponerse con carácter previo, potestativamente, recurso de reposición.

TÍTULO II. LA AGENCIA VASCA DE PROTECCIÓN DE DATOS

Artículo 10.- Creación y régimen jurídico - 1.-Se crea la Agencia Vasca de Protección de Datos como 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 esta ley y en su estatuto propio, que será aprobado por decreto del Gobierno Vasco a propuesta de la Vicepresidencia.

2.- La Agencia Vasca de Protección de Datos sujetará su actividad a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuando ejerza potestades administrativas. En el resto de su actividad se someterá a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en esta ley y en las disposiciones de desarrollo de las mismas.

3.- La Agencia Vasca de Protección de Datos estará sujeta al derecho público vigente en materia de adquisiciones patrimoniales y contratación. Sus bienes y derechos pertenecerán al patrimonio de la Comunidad Autónoma del País Vasco.

4.- La representación y defensa en juicio de la Agencia Vasca de Protección de Datos estará a cargo de los servicios jurídicos de la Administración de la Comunidad Autónoma del País Vasco, conforme a lo dispuesto en sus normas reguladoras.

Artículo 11.- Personal - 1.- Los puestos de trabajo de la Agencia Vasca de Protección de Datos serán desempeñados por funcionarios de las administraciones públicas e instituciones a que se refiere el artículo 2.1 de esta ley y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal estará obligado a guardar secreto respecto a los datos de carácter personal que conozca en el desarrollo de su función.

2.- El personal al servicio de la Agencia Vasca de Protección de Datos estará sometido a la normativa reguladora de la función pública en la Administración General de la Comunidad Autónoma. De conformidad con la misma, corresponde a la Agencia Vasca de Protección de Datos determinar el régimen de acceso a sus puestos de trabajo, los requisitos y las características de las pruebas de selección, así como la convocatoria, gestión y resolución de los procedimientos de provisión de puestos de trabajo y promoción profesional.

3.- Los puestos de trabajo que comporten el ejercicio de potestades públicas estarán reservados a personal funcionario.

Artículo 12.- Recursos - La Agencia Vasca 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 de la Comunidad Autónoma.
b) Las subvenciones y aportaciones que se concedan a su favor.
c) Los ingresos, ordinarios y extraordinarios, derivados del ejercicio de sus actividades.
d) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.
e) Cualesquiera otros que legalmente puedan serle atribuidos.

Artículo 13.- Presupuesto - La Agencia Vasca de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno Vasco para que sea integrado, con la debida independencia, en los Presupuestos Generales de la Comunidad Autónoma, de acuerdo con la legislación reguladora del régimen presupuestario de la Comunidad Autónoma del País Vasco. Estará sometida a esta legislación en lo relativo al régimen de modificación, ejecución y liquidación de su presupuesto, atendiendo a estos efectos a la naturaleza de la entidad; al régimen de contabilidad pública y al control económico financiero y de gestión del Departamento de Hacienda y Administración Pública de la Administración de la Comunidad Autónoma, sin perjuicio de la fiscalización de sus actividades económico-financieras y contables por el Tribunal Vasco de Cuentas Públicas.

Artículo 14.- Órganos de gobierno - Son órganos de gobierno de la Agencia Vasca de Protección de Datos el director, el Consejo Consultivo y aquellos otros que se establezcan en su estatuto propio.

Artículo 15.- El director - 1. El director de la Agencia Vasca de Protección de Datos dirige la agencia y ostenta su representación. Será nombrado por decreto del Gobierno Vasco, por un periodo de cuatro años.

2.- Ejercerá sus funciones con plena independencia y objetividad, y no estará sujeto a instrucción alguna en el desempeño de aquellas. No obstante, el director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.

3.- El director de la Agencia Vasca de Protección de Datos sólo cesará antes de la expiración de su periodo por alguna de las siguientes causas:

a) A petición propia.
b) Por separación, acordada por el Consejo de Gobierno, previa instrucción de expediente, en el que necesariamente será oído el 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 Vasca de Protección de Datos tendrá la consideración de alto cargo, quedará en la situación de servicios especiales si anteriormente estuviera desempeñando una función pública, y estará sometido al régimen de incompatibilidades de los altos cargos de la Administración de la Comunidad Autónoma.

Artículo 16.- El Consejo Consultivo - 1.- El director de la Agencia Vasca de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

a) Un representante del Parlamento Vasco, designado por éste.
b) Un representante de la Administración de la Comunidad Autónoma del País Vasco, designado por el Consejo de Gobierno.
c) Un representante de los territorios históricos, designado por éstos de común acuerdo.
d) Un representante de las entidades locales del ámbito territorial de la Comunidad Autónoma del País Vasco, designado por la asociación más representativa de las mismas en el citado ámbito territorial.
e) Dos expertos, uno en informática y otro en el ámbito de los derechos fundamentales, designados por la Universidad del País Vasco previa consulta a las corporaciones de derecho público de la Comunidad Autónoma del País Vasco.

2.- El Consejo Consultivo aprobará sus propias normas de organización y funcionamiento, en las que se preverán las figuras de presidente y secretario, así como el sistema para su elección o designación.

Artículo 17.- Funciones - 1. Son funciones de la Agencia Vasca de Protección de Datos, en relación con los ficheros a que se refiere el artículo 2.1 de esta ley y en el ámbito de las competencias de la Comunidad Autónoma del País Vasco:

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 las leyes y reglamentos.
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 legislación vigente en materia de protección de datos.
d) Atender las peticiones y reclamaciones formuladas por los afectados.
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 a los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a la legislación en vigor y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros cuando no se ajuste a dicha legislación, salvo en la que se refiera a transferencias internacionales de datos.
g) Ejercer la potestad sancionadora y, en su caso, proponer la iniciación de procedimientos disciplinarios contra quienes estime responsables de las infracciones tipificadas en el artículo 22 de esta ley, así como adoptar las medidas cautelares que procedan, salvo en lo que se refiera a las transferencias internacionales de datos. Todo ello en los términos previstos en esta 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 anualmente una relación de dichos ficheros con la información adicional que el director de la Agencia Vasca de Protección de Datos determine.

k) Redactar una memoria anual y remitirla a la Vicepresidencia del Gobierno Vasco.
l) Velar por el cumplimiento de las disposiciones que la legislación sobre 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 24.
m) Colaborar con la Agencia de Protección de Datos del Estado y entidades similares de otras comunidades autónomas en cuantas actividades sean necesarias para una mejor protección de la seguridad de los ficheros de datos de carácter personal y de los derechos de los ciudadanos en relación con los mismos.
n) Atender a las consultas que en materia de protección de datos de carácter personal le formulen las administraciones públicas, instituciones y corporaciones a que se refiere el artículo 2.1 de esta ley, así como otras personas físicas o jurídicas, en relación con los tratamientos de datos de carácter personal incluidos en el ámbito de aplicación de esta ley.
ñ) Cuantas otras le sean atribuidas por las leyes y reglamentos.

2.- A los efectos de las funciones a que se refiere el número anterior, la Agencia Vasca de Protección de Datos tendrá la consideración de autoridad de control, y la ley le garantiza la plena independencia y objetividad en el ejercicio de su cometido.

Artículo 18.- Registro de Protección de Datos - 1. Se crea el Registro de Protección de Datos, como órgano integrado en la Agencia Vasca de Protección de Datos en los términos que se establezcan en los estatutos de ésta.

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

a) Los ficheros a los que se refiere el artículo 2.1 de esta ley.
b) Las autorizaciones a las que se refiere la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
c) Los códigos tipo que afecten a los ficheros inscritos.
d) Los datos relativos a los ficheros inscritos que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3.- El Registro de Protección de Datos podrá denegar la inscripción solicitada cuando considere que la petición no se ajusta a derecho. En este caso, el director de la Agencia Vasca de Protección de Datos deberá requerir al solicitante para que efectúe las correcciones oportunas.

4.- Reglamentariamente se regulará el procedimiento de inscripción de los ficheros a los que se refiere el artículo 2.1 de esta ley en el Registro de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes, y demás extremos pertinentes.

5.- El Registro de Protección de Datos será de consulta pública y gratuita. Cualquier persona podrá conocer, recabando la información oportuna del citado registro, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento.

Artículo 19.- Potestad de inspección - 1. La Agencia Vasca de Protección de Datos, como autoridad de control, podrá inspeccionar los ficheros a los que se refiere el artículo 2.1 de esta ley, recabando cuanta información precise para el cumplimiento de su cometido. A tal efecto, podrá 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 datos, accediendo a los locales donde se hallen instalados.

2.- Los funcionarios que ejerzan la inspección a que se refiere el número anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos, y estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de sus funciones, incluso después de haber cesado en las mismas.

Artículo 20.- Requerimientos a los titulares de los ficheros - Cuando el director de la Agencia Vasca de Protección de Datos constate que el mantenimiento y uso de un determinado fichero incluido en el ámbito de aplicación de esta ley contraviene algún precepto de la misma o de las disposiciones que la desarrollen, podrá requerir a la administración pública, institución o corporación titular del fichero que adopte las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento. Si la administración requerida incumpliera el requerimiento formulado, el director de la Agencia Vasca de Protección de Datos, sin perjuicio de otras medidas que pueda adoptar de acuerdo con el artículo 17.f) de esta ley, podrá recurrir la resolución o la actitud omisiva adoptada por aquella administración, teniendo, a estos efectos, la condición de interesado.

TÍTULO III.
RÉGIMEN SANCIONADOR

Artículo 21.- Responsables - Los responsables de los ficheros a los que se refiere el artículo 2.1 de esta ley y los encargados de los tratamientos de los mismos estarán sujetos al régimen de infracciones y sanciones establecido en esta ley.

Artículo 22.- 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 Vasca 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 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 legalmente exigida.
e) Incumplir el deber de secreto legalmente establecido, salvo que constituya infracción grave.

3.-Son infracciones graves:
a) Proceder a la creación de ficheros, o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general publicada en el Boletín Oficial del País Vasco o en el del territorio histórico correspondiente.
b) 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 exigido.
c) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías legalmente establecidos o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.
d) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.
e) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente proceda cuando resulten afectados los derechos de las personas amparadas por la legislación de protección de datos de carácter personal.
f) 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 o a Hacienda pública, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.
g) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad.
h) No remitir a la Agencia Vasca de Protección de Datos las comunicaciones previstas en las leyes y reglamentos, así como no proporcionar a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquélla a tales efectos.
i) La obstrucción al ejercicio de la función inspectora.

j) No inscribir el fichero de datos de carácter personal en el Registro de Protección de Datos, cuando haya sido requerido para ello por el director de la Agencia Vasca de Protección de Datos.
k) Incumplir el deber de información legalmente establecido, 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 datos de carácter personal, fuera de los casos en que estén permitidas.
c) Recabar y tratar datos de carácter personal que revelen ideología, afiliación sindical, religión o creencias, cuando no medie consentimiento expreso del afectado.
d) Recabar y tratar datos referidos al origen racial, a la salud o a la vida sexual, cuando no lo disponga una ley o el afectado no haya consentido expresamente.
e) Crear ficheros 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.
f) 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 Vasca de Protección de Datos o por los titulares del derecho de acceso.
g) 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.
h) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hace referencia la letra e) de este mismo apartado, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.
i) No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
j) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

5.- La tipificación de infracciones que contiene este artículo se entiende sin perjuicio de las tipificadas en la legislación estatal sobre protección de datos, en aquellos aspectos sobre los que la Comunidad Autónoma del País Vasco carece de competencia.

Artículo 23.- Tipos de sanciones - 1. Las infracciones leves serán sancionadas con multa de 601,01 a 60.101,21 euros.

2.- Las infracciones graves serán sancionadas con multa de 60.101,21 a 300.506,05 euros.

3.- Las infracciones muy graves serán sancionadas con multa de 300.506,05 a 601.012,1 euros.

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

5.- Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquélla 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 Vasco actualizará periódicamente la cuantía de las sanciones, de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 24.- Infracciones cometidas por las administraciones públicas, instituciones y corporaciones de Derecho público - 1. Cuando, instruido el correspondiente procedimiento, se llegue a la conclusión de que se ha cometido alguna o algunas de las infracciones a que se refiere el artículo anterior, en relación con los ficheros a que se refiere el artículo 2.1 de esta ley, el director de la Agencia Vasca 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, y la misma agota la vía administrativa.

2.- El director de la Agencia Vasca de Protección de Datos podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán los establecidos en la legislación reguladora del régimen disciplinario de los funcionarios y personal al servicio de las administraciones públicas, instituciones y corporaciones a las que se refiere el artículo 2.1 de esta ley. A estos efectos, las infracciones tipificadas en esta ley completarán el régimen disciplinario que sea de aplicación.

3.- En el supuesto de que haya que seguir un procedimiento sancionador, se estará a lo dispuesto en la Ley 2/1998, de 20 de febrero, de la Potestad Sancionadora de las Administraciones Públicas de la Comunidad Autónoma del País Vasco.

4.- Se deberán comunicar a la Agencia Vasca de Protección de Datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los números anteriores.

5.- El director de la Agencia Vasca de Protección de Datos comunicará al Ararteko las actuaciones que efectúe y las resoluciones que dicte al amparo de los números anteriores.

Artículo 25.- 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 Vasca de Protección de Datos podrá requerir a los responsables de ficheros de datos de carácter personal la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

DISPOSICIONES ADICIONALES

Primera.- Comunicación de ficheros a la Agencia Vasca de Protección de Datos - Las administraciones públicas, instituciones y corporaciones a que se refiere el artículo 2.1) de esta ley comunicarán a la Agencia Vasca de Protección de Datos, en el plazo de tres meses a partir de la entrada en vigor de esta ley, los ficheros de datos de carácter personal señalados en aquel precepto que sean de su titularidad. Previamente deberán tener aprobada y publicada la disposición reguladora del correspondiente fichero.

Segunda.- Comunicación de datos del padrón - 1.-Las administraciones general y forales de la Comunidad Autónoma del País Vasco podrán solicitar al Euskal Estatistika-Erakundea/Instituto Vasco de Estadística, en los términos que se establecen en la disposición adicional segunda de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y artículo 17.3 de la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local, 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 correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población. Estos 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.

2.- A los efectos de lo dispuesto en el párrafo anterior, se modifica el artículo 29 de la Ley 4/1986, de 28 de abril, de Estadística de la Comunidad Autónoma de Euskadi, en los siguientes térmi-

nos: la redacción actual del citado precepto queda como número 1 del mismo, al que se añade un número 2 con el siguiente texto:

"2. El Euskal Estatistika-Erakundea/Instituto Vasco de Estadística actuará también como depositario de copias de los padrones municipales de todos los municipios de la Comunidad Autónoma del País Vasco, a cuyos efectos éstos le deberán remitir copias de los citados registros administrativos en los términos que se establezcan reglamentariamente".

Tercera.- Competencias del Ararteko y de la Agencia de Protección de Datos del Estado - Lo dispuesto en esta ley se entiende sin perjuicio de las competencias que tengan atribuidas el Ararteko y la Agencia de Protección de Datos del Estado.

DISPOSICIÓN FINAL
Desarrollo y aplicación

1.- Se autoriza al Gobierno Vasco para el desarrollo y aplicación de lo dispuesto en esta ley.

2.- Se autoriza al Departamento de Hacienda y Administración Pública para crear la sección presupuestaria correspondiente y para realizar, de acuerdo con la legislación reguladora del régimen presupuestario de la Comunidad Autónoma del País Vasco, las modificaciones presupuestarias precisas para la aplicación de lo dispuesto en esta ley.

Por consiguiente, ordeno a todos los ciudadanos y ciudadanas de Euskadi, particulares y autoridades, que la guarden y hagan guardarla.

4.2 DECRETO 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos.

(BOPV núm. 218, de 16 de noviembre de 2005)

Por Ley 2/2004, de 25 de febrero, se regulan aspectos relacionados con los ficheros de datos de carácter personal creados o gestionados por los Entes públicos de la Comunidad Autónoma del País Vasco y se crea la Agencia Vasca de Protección de Datos. Es preciso completar la regulación legal para una protección más eficaz de la intimidad personal y familiar de los ciudadanos, más concretamente, lo que la doctrina ha venido en denominar el derecho a la autodeterminación informativa; aunque, en este caso, la protección sólo se hace operativa en relación con ficheros vinculados, por su creación o por su gestión, a los Entes públicos de la Comunidad Autónoma del País Vasco. La misma Ley 2/2004, en su disposición final, autoriza al Gobierno Vasco para su desarrollo y aplicación. Pero, además de esta habilitación de carácter general, la Ley 2/2004 contiene diversas llamadas al reglamento, de entre las que debemos destacar la relativa a la regulación del procedimiento para el ejercicio de los derechos de oposición, acceso, rectificación, cancelación y cualesquiera otros que les reconozca la ley. Bien es cierto que el legislador ha querido que cada Ente público de la Comunidad Autónoma del País Vasco regule este procedimiento en relación con los ficheros de su titularidad (es decir, de los creados o gestionados por el mismo), por lo que este Decreto se limita a establecer reglas procedimentales para el ejercicio de tales derechos respecto de los ficheros creados o gestionados por la propia Administración autonómica. La Ley 2/2004 también remite al reglamento la regulación de las reclamaciones que los ciudadanos, a quienes se deniegue los derechos a que se refiere dicha Ley, pueden interponer ante la Agencia Vasca de Protección de Datos.

No aborda este Decreto los aspectos orgánicos de la Agencia Vasca de Protección de Datos, que son materia propia del Estatuto de este Ente, de acuerdo con el artículo 14 de la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos.

El Decreto consta de 19 artículos y una disposición final que habilita a la Vicepresidenta para el desarrollo del Decreto, previo informe del Consejo Consultivo de la Agencia Vasca de Protección de Datos. Aquéllos están distribuidos en cuatro capítulos.

El Capítulo I de disposiciones generales, concreta el ámbito de aplicación del Decreto y regula aspectos relacionados con la notificación de los ficheros a la Agencia Vasca de Protección de Datos y los códigos tipo.

El Capítulo II se refiere al ejercicio de los derechos en que se concreta la autodeterminación informativa, en la fase inicial; es decir, ante el responsable del fichero. Es de destacar que el ámbito de aplicación de este Capítulo se limita a los ficheros creados o gestionados por la Administración de la Comunidad Autónoma del País Vasco y Entes públicos vinculados o dependientes de la misma.

En el Capítulo III se regula el bloqueo de datos y la tutela de los derechos que integran el de autodeterminación informativa, en la fase de reclamación ante la Agencia Vasca de Protección de Datos, una vez que el ciudadano afectado ha visto desestimada su pretensión ante el responsable del fichero. Se regulan, asimismo, las diversas posibilidades de actuación inmediata de la Agencia Vasca de Protección de Datos, ante los responsables de los ficheros que incumplen los preceptos legales o reglamentarios, para proteger los derechos de los ciudadanos.

El Capítulo IV contiene preceptos relativos al procedimiento sancionador que ha de seguir la Agencia Vasca de Protección de Datos en relación con los ficheros que entran en su ámbito de

aplicación. Es necesario completar la regulación contenida en la Ley 2/2004, de acuerdo con la que se establece en la Ley 2/1998, de 20 de febrero, de la potestad sancionadora de las Administraciones Públicas de la Comunidad Autónoma del País Vasco. En este sentido, conviene recordar que la misma disposición adicional segunda del Real Decreto 1332/1994, de 20 de junio, de desarrollo de determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (vigente, al amparo de la disposición transitoria tercera de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal), atribuye a las Comunidades Autónomas, respecto de sus propios ficheros, la regulación del procedimiento sancionador, así como la del ejercicio y tutela de los derechos del afectado.

En su virtud, a propuesta de la Vicepresidenta del Gobierno, de conformidad con la Comisión Jurídica Asesora de Euskadi, y previa deliberación y aprobación del Consejo de Gobierno en su reunión celebrada el día 18 de octubre de 2005,

DISPONGO:

CAPÍTULO I - DISPOSICIONES GENERALES

Artículo 1.- Ámbito de aplicación. - 1.- El presente Decreto, salvo lo dispuesto en su Capítulo II que tendrá el ámbito de aplicación previsto en el mismo, será de aplicación a los siguientes ficheros:

Los creados por las Administraciones Públicas, Instituciones, Entidades y Corporaciones a las que se refiere el artículo 2.1 de la Ley 2/2004 (a las que, en adelante, se denominará Entes públicos de la Comunidad Autónoma del País Vasco) para el ejercicio de potestades de derecho público, que sean gestionados por las mismas o por personas, físicas o jurídicas, privadas.
Los creados por otras personas, físicas o jurídicas, públicas o privadas, en tanto sean gestionados por los Entes públicos de la Comunidad Autónoma del País Vasco para el ejercicio de potestades de derecho público.

2.- Lo dispuesto en este Decreto no será de aplicación a los ficheros a que se refiere el artículo 2.2 de la Ley 2/2004.

3.- Los ficheros de datos personales que sirvan para fines exclusivamente estadísticos, amparados por la legislación sobre función pública estadística, se regirán por sus disposiciones específicas, sin perjuicio de la aplicación de lo especialmente dispuesto para los mismos en este Decreto.

4.- Los ficheros de datos relativos a la salud de las personas, de la titularidad de instituciones y centros sanitarios de carácter público y de los profesionales a su servicio, se regirán por lo dispuesto en la legislación sectorial sobre sanidad, sin perjuicio de la aplicación de lo dispuesto en este Decreto en todo lo que no sea incompatible con dicha legislación.

5.- La aplicación de lo dispuesto en este Decreto a los ficheros de datos de carácter personal, distintos de los citados en el artículo 2.2 de la Ley 2/2004, creados o gestionados por los Cuerpos de Policía del País Vasco, se efectuará sin perjuicio de las especialidades de su régimen jurídico previstas en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en la Ley 4/1992, de 17 de julio, de Policía del País Vasco, y en las disposiciones que las desarrollen.

Artículo 2.- Notificación de ficheros a la Agencia Vasca de Protección de Datos. - 1.- Los Entes públicos de la Comunidad Autónoma del País Vasco notificarán a la Agencia Vasca de Protección de Datos toda creación, modificación o supresión de ficheros de datos de carácter personal, para su inscripción en el Registro de Protección de Datos, mediante el traslado, a través del modelo normalizado que al efecto elabore la Agencia Vasca de Protección de Datos, de una copia de la disposición o acuerdo de creación, modificación o supresión.

2.- Los Entes públicos de la Comunidad Autónoma del País Vasco notificarán a la Agencia Vasca de Protección de Datos, utilizando el modelo que al efecto elabore ésta, los ficheros a que se refiere el artículo 1.1.b de este Decreto que gestionen para el ejercicio de potestades de derecho público.

Artículo 3.- Los códigos tipo. - 1.- Los códigos tipo se depositarán, para su inscripción, en el Registro de Protección de Datos, de acuerdo con lo dispuesto en el Estatuto de la Agencia Vasca de Protección de Datos.

2.- Cualquier persona podrá obtener copias de los códigos tipo depositados e inscritos en el Registro de Protección de Datos.

3.- En caso de incumplimiento de las normas contenidas en los códigos tipo se estará a lo dispuesto al efecto en los acuerdos o disposiciones que los formulen.

CAPÍTULO II - EJERCICIO DE LOS DERECHOS, EN RELACIÓN CON LOS FICHEROS DE LA ADMINISTRACIÓN DE LA CAPV

Artículo 4.- Carácter personal de los derechos. - 1.- El derecho de oposición y el de acceso a los ficheros de datos de carácter personal creados o gestionados por la Administración de la Comunidad Autónoma del País Vasco y por los Entes públicos, de cualquier tipo, dependientes o vinculados a la misma, así como los derechos de rectificación y cancelación de datos, son personalísimos y serán ejercidos por el afectado frente al responsable del fichero, sin más limitaciones que las expresamente previstas en la Ley Orgánica 15/1999 y demás disposiciones en vigor. No obstante, podrá 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 derechos.

2.- Para el ejercicio de los derechos a que se refiere este artículo, por medio de representante voluntario, deberá acreditarse la representación, para cada actuación concreta, por cualquier medio válido en derecho que deje constancia fidedigna o mediante declaración en comparecencia personal del interesado ante el responsable del fichero.

Artículo 5.- Derecho de oposición. - 1.- Cuando el tratamiento de datos de carácter personal requiere el consentimiento inequívoco del afectado, el derecho de oposición se ejerce tanto mediante la no manifestación de dicho consentimiento como mediante la manifestación de la negativa a concederlo.

2.- En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de datos de carácter personal, y siempre que la ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal, mediante escrito dirigido al responsable del fichero. En tal supuesto, éste excluirá del tratamiento o tratamientos a que se refiera la petición, los datos relativos al afectado y le notificará a éste, en un plazo no superior a diez días, los términos en los que se ha efectuado la exclusión.

Artículo 6.- Derecho de acceso. - 1.- El derecho de acceso, a los ficheros de la Administración de la Comunidad Autónoma del País Vasco y Entes públicos dependientes o vinculados a la misma, se ejercerá mediante solicitud dirigida al responsable del fichero. Podrá formularse por cualquier medio que garantice la identificación del afectado y la constancia del fichero o ficheros a consultar.

2.- 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.

3.- El responsable del fichero resolverá sobre la petición de acceso en el plazo de un mes, a contar desde el día de la recepción de la solicitud. Transcurrido dicho plazo sin resolución expresa, el interesado podrá interponer la reclamación prevista en el artículo 9 de la Ley 2/2004.

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

Artículo 7.- Contenido de la información. - 1.- La información, cualquiera que sea el soporte en que fuera facilitada, se dará de forma legible o inteligible sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

2.- La información podrá comprender, de acuerdo con los términos de la petición, 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 8.- Denegación del acceso. - Sólo podrá denegarse el acceso cuando la solicitud sea formulada por persona distinta de la afectada o de su representante en los términos del artículo 4 de este Decreto, o se dé alguno de los supuestos de denegación previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Artículo 9.- Derechos de rectificación y cancelación. - 1.- Cuando el interesado considere que sus datos son inexactos o incompletos, inadecuados o excesivos podrá 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.

2.- La rectificación o cancelación se hará efectiva, por el responsable del fichero, dentro de los diez días siguientes al de la recepción de la solicitud. Si los datos hubieran sido comunicados a un tercero, el responsable del fichero le notificará, en el mismo plazo, la rectificación o cancelación efectuada, para que, en el caso de que aquél mantenga el tratamiento por cuenta de éste, proceda también a la misma rectificación o cancelación.

3.- En el supuesto de que el responsable del fichero considere que no procede acceder a lo solicitado por el afectado, se lo comunicará motivadamente, dentro del plazo señalado en el número anterior, a fin de que éste pueda hacer uso de la reclamación prevista en el artículo 9 de la Ley 2/2004 ante la Agencia Vasca de Protección de Datos.

4.- Transcurrido el plazo de diez días sin que se haya notificado expresamente la resolución, el interesado podrá formular la reclamación que corresponda ante la Agencia Vasca de Protección de Datos.

CAPÍTULO III - BLOQUEO DE DATOS Y TUTELA DE DERECHOS POR LA AGENCIA VASCA DE PROTECCIÓN DE DATOS

Artículo 10.- Bloqueo de los datos. - 1.- La cancelación de los datos dará lugar al bloqueo de los mismos, con el fin de impedir su ulterior proceso o utilización, 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.

2.- Cumplido el citado plazo se procederá a la supresión de los datos. No obstante, cuando los datos a cancelar hayan sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren.

3.- Contra la resolución por la que el responsable del fichero acuerda el bloqueo de los datos podrá interponerse, ante el Director de la Agencia Vasca de Protección de Datos, la reclamación prevista en el artículo 9 de la Ley 2/2004.

4.- A los efectos de lo dispuesto en este artículo, se entiende por bloqueo de datos la identificación y reserva de datos con el fin de impedir su tratamiento.

Artículo 11.- Tutela de derechos. - 1.- Las reclamaciones ante la Agencia Vasca de Protección de Datos, a que se refiere el artículo 9 de la Ley 2/2004, se sustanciarán en la forma prevista en este artículo.

2.- El procedimiento se iniciará a instancia del afectado o afectados, que deberá expresar, con claridad y por escrito, el contenido de la reclamación y los preceptos legales o reglamentarios que consideran vulnerados.

3.- Recibida la reclamación en la Agencia Vasca de Protección de Datos, se dará traslado de la misma al responsable del fichero, para que, en el plazo de 15 días, formule las alegaciones que estime pertinentes.

4.- Recibidas las alegaciones o transcurrido el plazo para formularlas, el Director de la Agencia Vasca de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del responsable del fichero y de los afectados, en los supuestos en que proceda, de acuerdo con el artículo 84 de la Ley 30/1992, resolverá sobre la reclamación formulada, dando traslado de la resolución a los interesados.

5.- Transcurridos seis meses, desde la presentación del escrito de reclamación, sin que se haya notificado resolución expresa, se entenderá que aquélla ha sido desestimada.

6.- Contra la resolución del Director de la Agencia Vasca de Protección de Datos o la desestimación por silencio administrativo de la tutela solicitada podrá interponerse recurso contencioso-administrativo, de acuerdo con la Ley reguladora de esta Jurisdicción. No obstante, podrá interponerse con carácter previo y potestativo recurso de reposición.

Artículo 12.- Requerimientos a los responsables de los ficheros - 1.- Cuando el Director de la Agencia Vasca de Protección de Datos constate que el mantenimiento o uso de un determinado fichero creado o gestionado por un Ente público de la Comunidad Autónoma del País Vasco contraviene un precepto legal o reglamentario podrá requerir al responsable del fichero que adopte las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento. Dentro de este plazo, si fuera igual o superior a cinco días, y en este último plazo si fuera inferior a él, el responsable del fichero podrá presentar las alegaciones que estime convenientes, vistas las cuales, en su caso, el Director de la Agencia Vasca de Protección de Datos adoptará la resolución que proceda, en un plazo no superior a otros cinco días.

2.- El requerimiento contendrá las medidas cautelares necesarias para garantizar los derechos de los ciudadanos afectados, así como también contendrá el acuerdo de inicio del procedimiento sancionador que corresponda. En este caso, el responsable del fichero podrá presentar alegaciones en el plazo de cinco días posteriores a la adopción de la medida cautelar.

3.- Si el responsable del fichero requerido incumpliera el requerimiento formulado o, en su caso, la resolución posterior al trámite de alegaciones, el Director de la Agencia Vasca de Protección de Datos podrá recurrir, la resolución o la actitud omisiva del responsable del fichero, ante la Jurisdicción Contencioso-Administrativa, de acuerdo con la Ley reguladora de esta Jurisdicción.

4.- Si el requerimiento se produce en el marco de un procedimiento sancionador y es para que cese una utilización o cesión ilícita de datos de carácter personal, constitutiva de infracción muy grave, 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 Vasca de Protección de Datos podrá adoptar las medidas cautela-

res a que se refiere este artículo. Además, si el requerimiento no fuera atendido en el plazo que se establezca, nunca superior a dos días, el Director de la Agencia Vasca de Protección de Datos podrá, mediante resolución motivada, inmovilizar los ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

Artículo 13.- Adopción de medidas cautelares por la Inspección de la Agencia Vasca de Protección de Datos. - 1.- Excepcionalmente, si para evitar la continuidad o la repetición de hechos de igual o similar significación que otros ya sancionados como muy graves; para evitar el mantenimiento de los daños que aquéllos hayan ocasionado, o para mitigar dichos daños, se requiere la asunción inmediata de medidas cautelares, éstas podrán ser impuestas, sin audiencia de los interesados, por funcionarios que en el ejercicio de las funciones de inspección atribuidas a la Agencia Vasca de Protección de Datos constaten los hechos eventualmente ilícitos. Dichas medidas cautelares, así como la causa y finalidad concreta de las mismas, deberán expresarse en el acta de inspección.

2.- Cuando se adopten las medidas cautelares a que se refiere el número anterior, el inspector actuante las pondrá inmediatamente en conocimiento del Director de la Agencia Vasca de Protección de Datos, el cual procederá a la incoación del correspondiente procedimiento sancionador. En el acto de iniciación se determinará, motivadamente, la revocación, mantenimiento o modificación de las citadas medidas cautelares, y se dará un plazo de cinco días, al responsable del fichero, para que formule las alegaciones que estime conveniente.

3.- Las medidas cautelares a que se refiere este artículo se extinguirán una vez transcurridos cuatro días desde su adopción sin que se haya iniciado el correspondiente procedimiento sancionador.

CAPÍTULO IV - PROCEDIMIENTO SANCIONADOR

Artículo 14.- Iniciación**. -** 1.- El procedimiento sancionador se iniciará de oficio por acuerdo del Director de la Agencia Vasca de Protección de Datos, bien por propia iniciativa, por petición razonada de una Administración Pública u otro Ente público o por denuncia.

2.- El acuerdo de iniciación contendrá, al menos: a) la identificación de la persona o personas presuntamente responsables; b) la descripción de los hechos que motivan la incoación del procedimiento, su posible calificación jurídica y las sanciones que pudieran corresponder; c) la designación del instructor del procedimiento, con expresa indicación del régimen de recusación; y d) la indicación de que el órgano competente para la resolución del procedimiento es el Director, con mención del precepto del Estatuto de la Agencia Vasca de Protección de Datos que le atribuye la competencia.

3.- El instructor será un funcionario Letrado de la Agencia Vasca de Protección de Datos, designado siguiendo un sistema objetivo de turno en el supuesto de que hubiera más de uno. No estará sujeto a dependencia funcional alguna en el cumplimiento de su labor instructora.

Artículo 15.- Instrucción**. -** 1.- El acuerdo de iniciación del expediente sancionador se comunicará al instructor y se notificará al presunto responsable y demás interesados, dándoles un plazo de quince días para aportar cuantas alegaciones, documentos o informaciones estimen convenientes, para solicitar la apertura de un período probatorio y proponer los medios de prueba que consideren adecuados.

2.- Se abrirá un período probatorio en los siguientes supuestos:
a) Cuando, en el trámite de alegaciones, lo solicite cualquiera de los interesados, con proposición de medios de prueba concretos, siempre que alguno de éstos sea considerado pertinente por el instructor. Éste deberá motivar, en su caso, la desestimación de la solicitud de apertura del período probatorio y el rechazo de pruebas concretas; actos que serán recurribles de acuerdo con el artículo 41 de la Ley 2/1998, de 20 de febrero, de la potestad sancionadora de las Administraciones Públicas de la Comunidad Autónoma del País Vasco.

b) Cuando, en ausencia de solicitud de parte interesada, el instructor lo considere necesario para el esclarecimiento de los hechos y determinación de los responsables. En este caso, dará un plazo de cinco días a los interesados para que propongan los medios de prueba que estimen oportunos.

3.- El período probatorio durará treinta días hábiles, sin perjuicio de la posibilidad de reducir o prorrogar dicho plazo en los supuestos legalmente previstos.

4.- La práctica de las pruebas se realizará de acuerdo con lo establecido en la Ley 30/1992.

Artículo 16.- Propuesta de resolución y trámite de audiencia. - 1.- Concluido, en su caso, el período probatorio, el instructor formulará la propuesta de resolución, de acuerdo con el artículo 38 de la Ley 2/1998, de 20 de febrero, de la potestad sancionadora de las Administraciones Públicas de la Comunidad Autónoma del País Vasco.

2.- La propuesta de resolución se notificará a los interesados, indicándoles que disponen de un plazo de quince días para formular alegaciones y que, en dicho plazo, se les pondrá de manifiesto el expediente, a fin de que puedan consultarlo y obtener copias de los documentos que obren en el mismo.

3.- Concluido el trámite de audiencia, el instructor cursará inmediatamente la propuesta de resolución al Director de la Agencia Vasca de Protección de Datos, junto con los documentos, alegaciones e informaciones que obren en el expediente.

Artículo 17.- Actuaciones complementarias. - Antes de dictar resolución, el Director de la Agencia Vasca de Protección de Datos podrá decidir, mediante acuerdo motivado, la realización de las actuaciones complementarias que considere necesarias para la resolución del procedimiento, de acuerdo con el artículo 42 de la Ley 2/1998.

Artículo 18.- Remisión a órgano competente. - Cuando, en cualquier fase del procedimiento sancionador, el Director de la Agencia Vasca de Protección de Datos considere que los hechos son constitutivos de una infracción cuya sanción no le compete, lo comunicará al órgano que considere competente, trasladándole todo lo actuado.

Artículo 19.- Resolución del procedimiento. - 1.- El Director de la Agencia Vasca de Protección de Datos dictará resolución motivada, que decidirá sobre todas las cuestiones planteadas por los interesados y aquellas otras derivadas del procedimiento, de acuerdo con el artículo 43 de la Ley 2/1998 y artículo 24 de la Ley 2/2004. Asimismo, contendrá la declaración pertinente en orden a las medidas provisionales o cautelares adoptadas durante la tramitación del procedimiento.

2.- Si no hubiera sido notificada la resolución en el plazo de seis meses desde la iniciación del procedimiento, se producirá la caducidad de éste, en los términos y con las consecuencias que establece la Ley 30/1992. No obstante, el referido plazo quedará interrumpido mientras el procedimiento se encuentre paralizado por causas imputables a los interesados, así como en el resto de los supuestos previstos en la Ley 2/1998.

DISPOSICIÓN FINAL
Desarrollo reglamentario.

Se faculta a la Vicepresidenta del Gobierno Vasco para, previo informe del Consejo Consultivo de la Agencia Vasca de Protección de Datos, desarrollar lo dispuesto en este Decreto.

4.3 Decreto 309/2005, de 18 de octubre, por el que se aprueba el Estatuto de la Agencia Vasca de Protección de Datos.

(BOPV núm. 213, de 9 de noviembre de 2005)

La Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, configura a ésta como 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. El artículo 10.1 de la citada Ley 2/2004 establece que la Agencia Vasca de Protección de Datos se regirá por lo dispuesto en la Ley de su creación y en su Estatuto propio que será aprobado por Decreto del Gobierno Vasco, a propuesta de la Vicepresidencia. Procede, en consecuencia, completar el diseño organizativo básico de la Agencia, previsto en la Ley 2/2004, mediante la aprobación de su Estatuto de acuerdo con las previsiones legales y dejando, al mismo tiempo, el margen de disponibilidad suficiente como para que la propia Agencia pueda ejercer las potestades de autoorganización necesarias para su adecuado funcionamiento, teniendo en cuenta, a estos efectos, que se trata de un ente que, en el ejercicio de las funciones que tiene legalmente atribuidas, actúa con plena independencia de las Administraciones Públicas.

En su virtud, a propuesta de la Vicepresidenta del Gobierno, de conformidad con la Comisión Jurídica Asesora de Euskadi, y previa deliberación y aprobación del Consejo de Gobierno en su reunión celebrada el día 18 de octubre de 2005,

DISPONGO:

Artículo único.- De conformidad con lo dispuesto en el artículo 10.1 de la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, se aprueba el Estatuto de esta Entidad, cuyo texto se inserta a continuación.

DISPOSICIÓN FINAL

Se autoriza a la Vicepresidenta del Gobierno Vasco y al Director de la Agencia Vasca de Protección de Datos, a cada uno en el ámbito de sus respectivas competencias, para el desarrollo y aplicación de lo dispuesto en el Estatuto de la Agencia Vasca de Protección de Datos.

ANEXO AL DECRETO 309/2005, DE 18 DE OCTUBRE

ESTATUTO DE LA AGENCIA VASCA DE PROTECCIÓN DE DATOS
CAPÍTULO I - DISPOSICIONES GENERALES

Artículo 1.- La Agencia Vasca de Protección de Datos. - La Agencia Vasca 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. La Agencia Vasca de Protección de Datos se relaciona con el Gobierno Vasco a través de la Vicepresidencia.

Artículo 2.- Régimen jurídico. - 1.- La Agencia Vasca de Protección de Datos se rige por las siguientes disposiciones legales y reglamentarias:

La Ley 2/2004 y las disposiciones reglamentarias de desarrollo de la misma.
El presente Estatuto.
La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y los reglamentos de desarrollo de la misma.

Cuando ejerza potestades administrativas, la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de la Administraciones Públicas y del Procedimiento Administrativo Común.
El Texto Refundido de las disposiciones legales vigentes sobre Régimen Presupuestario de Euskadi, aprobado por Decreto Legislativo 1/1994, de 27 de septiembre.
Cuantas otras disposiciones resulten de aplicación.

2.- La Agencia Vasca de Protección de Datos ejercerá sus funciones por medio del Director, a cuyos efectos, los actos del Director se consideran actos de la Agencia Vasca de Protección de Datos.

3.- Los actos dictados por el Director, en el ejercicio de las funciones públicas de la Agencia Vasca de Protección de Datos, agotan la vía administrativa. Contra los mismos podrá interponerse recurso contencioso-administrativo, sin perjuicio del previo recurso potestativo de reposición.

4.- La representación y defensa, en juicio, de la Agencia Vasca de Protección de Datos, estará a cargo de los servicios jurídicos de la Administración de la Comunidad Autónoma del País Vasco, de acuerdo con lo dispuesto en la Ley 7/1986, de 26 de junio, de Representación y Defensa de la Comunidad Autónoma del País Vasco.

CAPÍTULO II - FUNCIONAMIENTO DE LA AGENCIA VASCA DE PROTECCIÓN DE DATOS

Artículo 3.- Funciones de la Agencia Vasca de Protección de Datos. - La Agencia Vasca de Protección de Datos desempeñará las funciones que le atribuye el artículo 17 de la Ley 2/2004, para lo cual podrá dirigirse directamente a los responsables de los ficheros a que se refiere el artículo 2.1 de dicha Ley y a los encargados de tratamiento de los mismos.

Artículo 4.- Instrucciones y recomendaciones. - La Agencia Vasca de Protección de Datos velará por el cumplimiento de la legislación sobre protección de datos y controlará su aplicación, en relación con los ficheros a que se refiere el artículo 2.1 de la Ley 2/2004 y en el ámbito de las competencias autonómicas. A tal efecto dictará las instrucciones y recomendaciones necesarias para la correcta aplicación de las disposiciones legales y reglamentarias en materia de protección de datos de carácter personal, control de acceso a los ficheros y para adecuar los tratamientos de datos a lo dispuesto en las mismas.

Artículo 5.- Ficheros estadísticos. - En el ejercicio de las funciones que le atribuye el artículo 17.1.l de la Ley 2/2004, la Agencia Vasca de Protección de Datos dictará las instrucciones precisas para velar por el cumplimiento de las disposiciones que la legislación sobre función estadística establece respecto a la recogida de datos y al secreto estadístico. Asimismo, ejercerá, en esta materia, las siguientes funciones:

Informar las disposiciones normativas que determinen estadísticas de respuesta obligatoria.
Dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos.
Cualesquiera otras que la atribuyan las leyes y los reglamentos.

CAPÍTULO III - ORGANIZACIÓN DE LA AGENCIA VASCA DE PROTECCIÓN DE DATOS

Artículo 6.- Organización de la Agencia Vasca de Protección de Datos. 1.- La Agencia Vasca de Protección de Datos se estructura en los siguientes órganos:

El Director.
El Consejo Consultivo.

2.- Dependerán jerárquicamente del Director el Registro de Protección de Datos y otros órganos que se creen en virtud del presente Estatuto así como de las disposiciones que lo desarrollen.

Artículo 7.- El Director. - 1.- El Director de la Agencia Vasca de Protección de Datos dirige ésta y ostenta su representación.

2.- Corresponde al Director de la Agencia Vasca de Protección de Datos dictar las resoluciones, instrucciones y recomendaciones que requiera el ejercicio de las funciones de la Agencia Vasca de Protección de Datos y, en especial:

Resolver motivadamente sobre la procedencia o improcedencia de las inscripciones y demás anotaciones en el Registro de Protección de Datos.
Resolver las reclamaciones que le pueda dirigir la ciudadanía en el ejercicio de sus derechos de acceso, oposición, rectificación y cancelación, todo ello en relación con los ficheros de datos de carácter personal sujetos a la Ley 2/2004.
Recabar de las Administraciones Públicas, Instituciones, Entidades y Corporaciones a que se refiere el artículo 2.1 de la Ley 2/2004, la información necesaria para el cumplimiento de sus funciones.
Adoptar las medidas cautelares y provisionales que requiera el ejercicio de la potestad sancionadora, de conformidad con lo dispuesto en la Ley 2/2004.
Iniciar y resolver los expedientes sancionadores y, en su caso, instar la incoación de los expedientes disciplinarios en los casos de infracciones cometidas por Administraciones Públicas u otras Entidades o Instituciones de derecho público.
Autorizar la entrada en los locales en que se hallen los ficheros, con el fin de proceder a las inspecciones pertinentes. Cuando dichos locales tengan la consideración legal de domicilio, la labor inspectora deberá ajustarse, además, a las reglas que garantizan su inviolabilidad.
Actuar como órgano de contratación de la Agencia Vasca de Protección de Datos.
Aprobar gastos y ordenar pagos, dentro de los límites de los créditos del presupuesto de gastos de la Agencia Vasca de Protección de Datos.
Programar la gestión de la Agencia Vasca de Protección de Datos.
Elaborar el anteproyecto de presupuesto de la Agencia Vasca de Protección de Datos.
Elaborar y aprobar la relación de puestos de trabajo de la Agencia Vasca de Protección de Datos.
Aprobar la memoria anual de la Agencia Vasca de Protección de Datos y elevarla a la Vicepresidencia.
Firmar convenios de colaboración, con entidades públicas y privadas, para un mejor desempeño de las funciones atribuidas a la Agencia Vasca de Protección de Datos.
Dispensar al responsable del fichero, de la obligación de informar a los interesados, cuando concurran los supuestos previstos en el artículo 6 de la Ley 2/2004.
Instar a las Administraciones Públicas, Instituciones y Entidades a que se refiere el artículo 16 de la Ley 2/2004 a que designen, cuando proceda, a sus representantes en el Consejo Consultivo, a fin de evitar, en lo posible, la existencia de vacantes.
Cualesquiera otras que se le atribuyan en el presente Estatuto y demás disposiciones en vigor, así como todas aquellas funciones de dirección y representación de la Agencia Vasca de Protección de Datos que no estén expresamente atribuidas a otro órgano.

3.- El Director de la Agencia Vasca de Protección de Datos podrá delegar las funciones a que se refieren las letras g), h), i), j) y m) del número anterior en un órgano jerárquicamente dependiente del mismo.

4.- El Director de la Agencia Vasca de Protección de Datos percibirá las retribuciones que en los Presupuestos Generales de la Comunidad Autónoma del País Vasco tengan asignados los Directores de la Administración General de la Comunidad Autónoma del País Vasco.

5.- Cuando proceda tramitar el expediente que puede conducir a la separación del Director de la Agencia Vasca de Protección de Datos, por alguna de las causas previstas en el artículo 15.3.b de la Ley 2/2004, el acto de inicio y la elevación a Consejo de Gobierno de la propuesta de resolución del expediente corresponderán a la Vicepresidenta.

Artículo 8.- El Consejo Consultivo. - 1.- El Consejo Consultivo de la Agencia Vasca de Protección de Datos es un órgano colegiado de asesoramiento al Director de la Agencia Vasca de Protección de Datos, cuya composición es la que determina el artículo 16 de la Ley 2/2004.

2.- El Consejo Consultivo emitirá informe en todas las cuestiones que le someta el Director de la Agencia Vasca de Protección de Datos y podrá formular propuestas en temas relacionados con las materias de la competencia de ésta.

3.- Las personas designadas como miembros del Consejo Consultivo, comenzarán a desempeñar sus funciones a partir del día en que sea notificada la designación a la Secretaría del Consejo Consultivo.

4.- Los miembros del Consejo Consultivo desempeñarán su cargo durante el tiempo que se establezca en el acto o acuerdo de su designación, entendiéndose que ésta es por tiempo indefinido a falta de mención expresa a la duración.

5.- El Consejo Consultivo aprobará sus propias normas de organización y funcionamiento, de acuerdo con el artículo 16.2 de la Ley 2/2004 y artículos 22 a 27 de la Ley 30/1992.

Artículo 9.- Registro de Protección de Datos. - 1.- Serán objeto de inscripción en el Registro de Protección de Datos:

Los ficheros a que se refiere el artículo 2.1 de la Ley 2/2004.
Las autorizaciones a que se refiere la Ley Orgánica 15/1999 y disposiciones de desarrollo.
Los códigos tipo que afecten a los ficheros inscritos.

2.- En los asientos de inscripción de los ficheros creados por las Administraciones Públicas, Instituciones, Entidades y Corporaciones a que se refiere el artículo 2.1 de la Ley 2/2004, figurará, en todo caso, la información contenida en la disposición o acuerdo de creación o de modificación del fichero, con especificación de la disposición o acuerdo y del diario oficial de su publicación y toda aquella que sea necesaria para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3.- Los asientos de inscripción de los ficheros a que se refiere el número anterior, los de modificación de su contenido y los de cancelación de los mismos, se efectuarán de oficio, una vez publicadas las disposiciones o acuerdos de creación o de modificación, anotándose las incidencias de cualquier naturaleza que concurran en los ficheros inscritos. Lo dispuesto en este número se entiende sin perjuicio de la obligación, del titular del fichero, de notificar a la Agencia Vasca de Protección de Datos la creación, modificación o supresión del fichero, mediante el traslado de la correspondiente disposición o acuerdo, siguiendo el modelo normalizado que al efecto elabore la Agencia Vasca de Protección de Datos.

4.- En los asientos de inscripción de ficheros de titularidad privada gestionados, para el ejercicio de potestades de derecho público, por las Administraciones Públicas, Instituciones, Entidades y Corporaciones a que se refiere el artículo 2.1 de la Ley 2/2004, figurará toda la información que, respecto de los mismos ficheros, figura en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos. La inscripción de estos ficheros se practicará a solicitud del ente gestor y previa instrucción del oportuno expediente, en el que se dará audiencia al titular del fichero y se aportará, en su caso, el correspondiente certificado del Registro General de Protección de Datos.

5.- Los códigos tipo se depositarán, para su inscripción, en el Registro de Protección de Datos. Si se ajustan a las disposiciones vigentes, el Director de la Agencia Vasca de Protección de Datos resolverá su inscripción; en caso contrario, requerirá a los solicitantes para que subsanen las deficiencias en un plazo de diez días, con indicación de que, si así no lo hicieran, se les tendrá por desistidos de su petición, de acuerdo con el artículo 71 de la Ley 30/1992.

6.- Corresponde al Registro de Protección de Datos:

Instruir los expedientes de inscripción a que se refiere el artículo 18.2 de la Ley 2/2004.
Instruir los expedientes de modificación y cancelación del contenido de los asientos.
Rectificar de oficio los errores materiales de los asientos.
Expedir certificaciones de los asientos.
Publicar anualmente la relación de los ficheros inscritos, con la información adicional que el Director de la Agencia Vasca de Protección de Datos determine.

7.- El responsable del fichero que considere que la información relativa a éste, contenido del Registro de Protección de Datos, es incorrecta podrá presentar la oportuna reclamación ante el Director de la Agencia Vasca de Protección de Datos, que deberá resolverla en el plazo de un mes. Transcurrido este plazo sin que se haya notificado la resolución se entenderá estimada la reclamación y deberá modificarse el contenido del asiento en los términos de aquélla.

8.- Las resoluciones del Director de la Agencia Vasca de Protección de Datos que modifiquen el contenido del Registro de Protección de Datos serán notificadas a los responsables de los ficheros afectados. Contra las mismas podrá interponerse recurso contencioso-administrativo y, potestativamente, con carácter previo, el de reposición.

9.- El Director de la Agencia Vasca de Protección de Datos adoptará las medidas necesarias para facilitar el acceso de los ciudadanos al Registro de Protección de Datos.

10.- Al frente del Registro de Protección de Datos existirá un responsable directamente dependiente del Director de la Agencia Vasca de Protección de Datos. Éste podrá delegar en aquél la totalidad o parte de las funciones que le atribuye el presente artículo.

Artículo 10.- Otros órganos. - La estructura orgánica de la Agencia Vasca de Protección de Datos se completa con los órganos jerárquicamente dependientes del Director dedicados al desempeño de las funciones de asesoría, instrucción, inspección, secretaría y registro.

En desarrollo de dicha estructura orgánica, por resolución del Director, previo informe del Consejo Consultivo, se podrá prever la existencia de otras unidades funcional y jerárquicamente dependientes del Director, así como las funciones asignadas a las mismas. En la relación de puestos de trabajo se determinará la dotación de puestos de cada uno de los distintos órganos y unidades, las características de cada uno de los puestos y los requisitos exigidos para acceder a los mismos.

CAPÍTULO IV - INSPECCIÓN

Artículo 11.- Funciones inspectoras. - 1.- La Agencia Vasca de Protección de Datos podrá efectuar inspecciones periódicas o circunstanciales, de oficio o a instancia de los afectados, de cualesquiera de los ficheros a que se refiere el artículo 2.1 de la Ley 2/2004, se hallen o no inscritos en el Registro de Protección de Datos, y de los equipos informáticos correspondientes, en los locales que se hallen. A tal efecto podrá:

Examinar los soportes de información que contengan los datos personales.
Examinar los equipos físicos.
Requerir los programas o la documentación pertinente al objeto de determinar, en caso necesario, el tratamiento de que los datos sean objeto.
Examinar los sistemas de transmisión y acceso a los datos.
Realizar auditorías de los sistemas informáticos, para determinar su conformidad o no con la legislación vigente.
Requerir la exhibición de cualesquiera otros documentos pertinentes.
Requerir el envío de toda la información precisa para el ejercicio de las funciones inspectoras.
Revisar las medidas de seguridad aplicadas a los ficheros.

2.- Las funciones inspectoras serán desempeñadas por funcionarios adscritos a los puestos de inspector en la relación de puestos de trabajo de la Agencia Vasca de Protección de Datos, los cuales tendrán acceso a los locales en que se hallen los ficheros y los equipos informáticos, previa exhibición, al responsable del fichero, de la autorización expedida por el Director de la Agencia Vasca de Protección de Datos. Cuando dichos locales tengan la consideración legal de domicilio, la labor inspectora deberá ajustarse, además, a las reglas que garantizan su inviolabilidad.

Artículo 12.- Actos de instrucción de expedientes sancionadores. - Los funcionarios adscritos a los puestos de inspector colaborarán en los actos de instrucción de expedientes sancionadores tramitados por la Agencia Vasca de Protección de Datos.

CAPÍTULO V - RÉGIMEN ECONÓMICO, PATRIMONIAL Y DE PERSONAL

Artículo 13.- Recursos, contabilidad, control y presupuestos. - 1.- La Agencia Vasca de Protección de Datos contará, para el cumplimiento de sus fines, con los recursos previstos en el artículo 12 de la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

2.- Los regímenes presupuestario, contable y de control económico financiero y de gestión de la Agencia Vasca de Protección de Datos serán los previstos en el artículo 13 de la citada Ley 2/2004 y en las disposiciones específicas que sean de aplicación de acuerdo con dicho precepto. Asimismo de conformidad con el artículo 10.3 de dicha Ley el régimen de contratación de la Agencia Vasca de Protección de Datos será el previsto en el derecho público vigente para las Administraciones Públicas.

Artículo 14.- Régimen patrimonial. - 1.- Los bienes y derechos de la Agencia Vasca de Protección de Datos pertenecerán al patrimonio de la Comunidad Autónoma del País Vasco.

2.- Los bienes que la Administración de la Comunidad Autónoma del País Vasco adscriba a la Agencia Vasca de Protección de Datos quedarán afectados a su servicio y conservarán la calificación jurídica originaria. Estos bienes sólo podrán ser utilizados para los fines que determinaron su adscripción.

Artículo 15.- Régimen de personal. - 1.- La relación de puestos de trabajo de la Agencia Vasca de Protección de Datos será aprobada por Resolución de su Director, previo informe del Consejo Consultivo, y entrará en vigor el día de su publicación en el Boletín Oficial del País Vasco.

2.- Los puestos de inspector y cualesquiera otros que comporten el ejercicio de potestades públicas estarán reservados a personal funcionario.

3.- Los puestos reservados a funcionario se proveerán por concurso o por libre designación, previa convocatoria del Director de la Agencia Vasca de Protección de Datos, a la que podrán acceder funcionarios de las Administraciones Públicas, Instituciones y Entidades a que se refiere el artículo 2.1 de la Ley 2/2004 que cumplan los requisitos exigidos, para cada puesto, en la relación de puestos. No obstante, ésta podrá reservar determinados puestos de trabajo a funcionarios de la propia Agencia Vasca de Protección de Datos.

DISPOSICIONES ADICIONALES

Primera.- El Director de la Agencia Vasca de Protección de Datos incorporará al Registro de Protección de Datos los ficheros a que se refiere el artículo 2.1 de la Ley 2/2004 que ya estén creados, en la medida que vaya recibiendo las comunicaciones a que se refiere la disposición adicional primera de dicha Ley. Asimismo, podrá solicitar del Registro General de Protección de Datos de la Agencia Española de Protección de Datos la relación de ficheros y demás elementos inscritos en la misma que deben ser también objeto de inscripción en el Registro de Protección de Datos de la Agencia Vasca de Protección de Datos. En este último caso, la inscripción se practicará, en su caso, tras un trámite de audiencia, por un plazo de diez días, al responsable del fichero afectado; y la resolución que se adopte será notificada también al Registro General de Protección de Datos.

Segunda.- El Director de la Agencia Vasca de Protección de Datos designará a un funcionario al servicio de esta Entidad para que desempeñe las funciones de Secretario del Consejo Consultivo hasta que este órgano apruebe sus propias normas de organización y funcionamiento. Se podrá proceder a la constitución del primer Consejo Consultivo a partir del momento en que se reciba, en la Secretaría del Consejo, las notificaciones de designación de cuatro de sus miembros.

4.4 RESOLUCIÓN de 21 de julio de 2005, del Director de la Agencia Vasca de Protección de Datos, por la que se establecen los modelos normalizados y los medios por los que debe procederse a la solicitud de las inscripciones de creación, modificación o supresión de ficheros en el Registro de Protección de Datos de la Agencia Vasca de Protección de Datos.

(BOPV núm. 165, de 31 de agosto de 2005)

El artículo 18 de la Ley del Parlamento Vasco 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, crea el Registro de Datos y establece que serán objeto de inscripción en la misma los ficheros a los que se refiere el artículo 2.1 de dicha Ley.

Dicho Registro se convierte así en un instrumento esencial para el efectivo cumplimiento de las funciones que a la Agencia Vasca de Protección de Datos le vienen atribuidas por la Ley.

De la misma manera resultará ser vehículo fundamental para dar plena efectividad a los principios de publicidad, interconexión y mutua información que rigen las relaciones entre las diferentes Autoridades de Control, estatal y autonómicas y que ya han tenido una primera expresión con la firma del Protocolo de Colaboración para la puesta en marcha del Sistema de Información de Intercambio Registral (SIDIR).

Teniendo en cuenta que las Administraciones Públicas deben impulsar el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos y que los programas y aplicaciones que vayan a ser utilizados deben ser previamente aprobados y difundidas públicamente sus características, así como la existencia de un Plan estratégico de administración y gobierno electrónicos que tiene como objetivo, entre otros, el impulso y avance de la e-Administración Vasca a fin de mejorar la relación de ésta con los ciudadanos, en virtud de las facultades que la Ley 2/2004 de 25 de febrero atribuye a esta Agencia, el Director

RESUELVE:

Artículo 1. Aprobación de modelos y soportes. - 1. Aprobar los modelos normalizados de solicitud, tanto en soporte papel como en soporte digital, de inscripción de ficheros de datos de carácter personal creados o gestionados para el ejercicio de potestades públicas por las Administraciones Públicas, Instituciones, Corporaciones y Entes Públicos a que se refiere el artículo 2.1 de la ley 2/2004.

Artículo 2. Contenido de los modelos. 1.– Estos modelos están compuestos por:
– Una hoja de solicitud de inscripción, en la forma prevista en el anexo I.
– Un formulario de notificación del fichero, conforme a lo dispuesto en el anexo II, en las que se hará constar la información contenida en la disposición o acuerdo de creación o modificación del fichero y toda aquella necesaria para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Artículo 3. Obtención y tramitación de los modelos en soporte papel. - 1. Los modelos normalizados de solicitud de inscripción en soporte papel se podrán obtener gratuitamente en la Sede de la Agencia Vasca de Protección de Datos o podrán descargarse de la página Web de la misma.

2.– Los modelos normalizados de solicitud de inscripción en soporte papel convenientemente cumplimentados y firmados deberán ser presentados en el Registro de Protección de Datos de la Agencia Vasca de Protección de Datos o en cualquiera de los registros u oficinas públicas a las

que se refiere el artículo 38.4 de la Ley 30/1992 de 30 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
En este último caso, el responsable del Registro de Protección de Datos dirigirá, en el plazo de diez días desde la recepción, comunicación informando de la fecha en la que el impreso normalizado ha tenido entrada en dicho Registro.

Artículo 4. Obtención y tramitación de modelos en soporte digital. - 1. Se aprueba el diseño normalizado de los modelos en soporte digital de la solicitud de inscripción de ficheros de datos de carácter personal a los que se refiere el artículo 2 de la Ley 2/2004, de 25 de febrero, que se ajunta como en el anexo III de la presente Resolución. La Agencia Vasca de Protección de Datos facilitará un programa informático para la generación de solicitudes de inscripción que podrá descargarse desde la página Web de dicha Agencia.

2. El programa al que se alude en el apartado anterior permitirá generar un fichero con la documentación de inscripción. Este fichero se remitirá a la agencia, bien directamente a través de Internet, bien mediante un soporte digital que deberá ser el que se establece en el anexo IV.
En ambos casos deberá cumplimentarse y firmarse la hoja de solicitud de inscripción generada por el programa, que habrá de presentarse en el Registro de Protección de Datos de la Agencia Vasca de Protección de Datos o en cualquiera de los registros u oficinas públicas a las que se refiere el artículo 38.4 de la Ley 30/1992 de 30 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
El envío de la solicitud de la inscripción de los ficheros se ajustará a lo previsto en el anexo IV.

Artículo 5. Actualización de anexos. Las actualizaciones de los anexos consecuencias de avances tecnológicos, cambios formales y otras modificaciones accesorias serán realizadas a través de la página Web de la Agencia.

Artículo 6. Firma electrónica. Cuando esté disponible el uso de la firma electrónica avanzada para la Instituciones, Órganos, Corporaciones, Entes y Organismos responsables en cada caso, la remisión de la hoja de solicitud de inscripción se podrá realizar a través de Internet.

Artículo 7. Subsanación de errores y presentación de documentación complementaria.
Si en la solicitud de inscripción o en las hojas del formulario de notificación del fichero, ya sea en soporte papel o en digital existieran defectos o errores que impidieran tramitarla o no se ajustasen al diseño y demás especificaciones establecidas en esta Resolución, se requerirá al solicitante para que en el plazo de diez días subsane los mismos. Del mismo modo se actuará en el supuesto de recibirse a través de Internet el formulario de notificación y no recibirse la hoja de solicitud de inscripción conforme a lo prevenido en el apartado anterior.
Si transcurrido dicho plazo, los defectos o errores no han sido corregidos se entenderá desistido de su solicitud.

Artículo 8. Entrada en vigor.
La presente Resolución entrará en vigor al día siguiente de su publicación en el Boletín Oficial del País Vasco.

4.5 RESOLUCIÓN de 28 de noviembre de 2005, del Director de la Agencia Vasca de Protección de Datos por la que se desarrolla la estructura orgánica de la Agencia Vasca de Protección de Datos.

(BOPV núm. 247, de 29 de diciembre de 2005)

La Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, configura a ésta como 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.

El artículo 10.1 de la citada Ley 2/2004 establece que la Agencia Vasca de Protección de Datos se regirá por lo dispuesto en su Ley de creación y en su Estatuto propio que ha sido aprobado por Decreto 309/2005, de 18 de octubre.

El mencionado Estatuto establece el diseño organizativo básico de la Agencia, dejando, al mismo tiempo, el margen de disponibilidad suficiente como para que la propia Agencia pueda ejercer las potestades de autoorganización necesarias para su adecuado funcionamiento. Así, en su artículo 10 se concreta que «la estructura orgánica de la Agencia Vasca de Protección de Datos se completa con los órganos jerárquicamente dependientes del Director dedicados al desempeño de las funciones de asesoría, instrucción, inspección, secretaría y registro» y que «en desarrollo de dicha estructura orgánica, por resolución del Director, previo informe del Consejo Consultivo, se podrá prever la existencia de otras unidades funcional y jerárquicamente dependientes del Director, así como las funciones asignadas a las mismas».

Por otra parte, la Agencia Vasca de Protección de Datos, como prestadora de un servicio público, se ajustará a los siguientes criterios de actuación:
1.– Evaluará la calidad en la prestación del servicio, mediante el establecimiento y seguimiento de indicadores y la realización de encuestas de opinión y grado de satisfacción de usuarios (tanto de los ciudadanos como de las administraciones).
2.– Mostrará especial interés en coordinarse eficazmente con las Administraciones Públicas y con el resto de autoridades de control en protección de datos.
3.– Potenciará la simplificación y documentación de todos los procedimientos, facilitando la realización de gestiones a través de herramientas informáticas y de la utilización de la red.
4.– Facilitará el aprendizaje organizacional y premiará la excelencia entre sus trabajadores, fomentando la competencia y la formación entre los mismos.
5.– Dará una importancia fundamental al comportamiento proactivo, ayudando a las administraciones en el cumplimiento de la legislación y en el establecimiento de una nueva cultura en protección de datos.
Nace por tanto esta norma para desarrollar la estructura orgánica de la Agencia Vasca de Protección de Datos con carácter previo a la realización de los procesos necesarios para la elaboración de la Relación de Puestos de Trabajo.
En su virtud, de acuerdo con el Consejo Consultivo,

RESUELVO:

Primero.– Funciones. - La Agencia Vasca de Protección de Datos desempeñará las funciones que le atribuye el artículo 17 de la Ley 2/2004, para lo cual podrá dirigirse directamente a los responsables de los ficheros a que se refiere el artículo 2.1 de dicha Ley y a los encargados de tratamiento de los mismos.

Segundo.– Estructura orgánica de la Agencia Vasca de Protección de Datos. - 1.– Para el ejercicio de las funciones señaladas en el artículo anterior, la Agencia Vasca de Protección de Datos se estructura en los siguientes órganos:

a) Órgano Unipersonal.

a.1.– Director o Directora.

b) Órgano Colegiado.

b.1.– El Consejo Consultivo, en los términos previstos en la Ley.

2.– Las Unidades administrativas jerárquicamente dependientes del Director o Directora son:

a) Registro de Protección de Datos y Nuevas Tecnologías.

b) Asesoría Jurídica e Inspección.

c) Secretaría General.

Tercero.– El Director o Directora. - 1.– El Director o Directora de la Agencia Vasca de Protección de Datos dirige esta y ostenta su representación. En su ámbito interno, ejerce la dirección, coordinación y control de todas las unidades administrativas jerárquicamente dependientes del mismo.

2.– Corresponde asimismo al Director o Directora dictar las resoluciones, instrucciones y recomendaciones que requiera el ejercicio de las funciones de la Agencia Vasca de Protección de Datos y, en especial:

a) Resolver motivadamente sobre la procedencia o improcedencia de las inscripciones y demás anotaciones en el Registro de Protección de Datos.

b) Resolver las reclamaciones que le pueda dirigir la ciudadanía en el ejercicio de sus derechos de acceso, oposición, rectificación y cancelación, todo ello en relación con los ficheros de datos de carácter personal sujetos a la Ley 2/2004.

c) Recabar de las Administraciones Públicas, Instituciones, Entidades y Corporaciones a que se refiere el artículo 2.1 de la Ley 2/2004, la información necesaria para el cumplimiento de sus funciones.

d) Adoptar las medidas cautelares y provisionales que requiera el ejercicio de la potestad sancionadora, de conformidad con lo dispuesto en la Ley 2/2004.

e) Iniciar y resolver los expedientes sancionadores y, en su caso, instar la incoación de los expedientes disciplinarios en los casos de infracciones cometidas por Administraciones Públicas, Instituciones, Entidades y Corporaciones.

f) Autorizar la entrada en los locales en que se hallen los ficheros, con el fin de proceder a las inspecciones pertinentes. Cuando dichos locales tengan la consideración legal de domicilio, la labor inspectora deberá ajustarse, además, a las reglas que garantizan su inviolabilidad.

g) Actuar como órgano de contratación de la Agencia Vasca de Protección de Datos.

h) Aprobar gastos y ordenar pagos, dentro de los límites de los créditos del presupuesto de gastos de la Agencia Vasca de Protección de Datos y conforme a los procedimientos que se establezcan internamente.

i) Aprobar el anteproyecto de presupuesto de la Agencia Vasca de Protección de Datos.

j) Programar la gestión de la Agencia Vasca de Protección de Datos, dirigir el plan estratégico y coordinar los planes de gestión y el seguimiento de los mismos.

k) Elaborar y aprobar la relación de puestos de trabajo de la Agencia Vasca de Protección de Datos.

l) Convocar y resolver los procedimientos de provisión ordinarios de concurso de méritos y libre designación de los puestos de trabajo del personal funcionario adscritos a la Agencia, y también las comisiones de servicio cuando afecten a funcionarios de las Administraciones Públicas, Instituciones, Entidades y Corporaciones del artículo 2.1 de la Ley 2/2004.

m) Convocar y resolver los procedimientos de selección y promoción profesional del personal laboral adscrito a la Agencia.

n) Aprobar la memoria anual de la Agencia Vasca de Protección de Datos y elevarla a la Vicepresidencia.

o) Firmar convenios de colaboración, con entidades públicas y privadas, para un mejor desempeño de las funciones atribuidas a la Agencia Vasca de Protección de Datos.

p) Dispensar al responsable del fichero, de la obligación de informar a los interesados, cuando concurran los supuestos previstos en el artículo 6 de la Ley 2/2004.

q) Instar a las Administraciones Públicas, Instituciones, Entidades y Corporaciones a que se refiere el artículo 16 de la Ley 2/2004 a que designen, cuando proceda, a sus representantes en el Consejo Consultivo, a fin de evitar, en lo posible, la existencia de vacantes.

r) Aprobar los informes y las respuestas a consultas que sean planteados por las Administraciones Públicas, Instituciones, Entidades y Corporaciones a que se refiere el artículo 2.1 de la Ley 2/2004, y otras personas físicas o jurídicas, con el objeto de interpretar y aplicar la legislación en materia de protección de datos.

s) Colaborar con la Agencia Española de Protección de Datos y, a tal efecto, acordar la remisión periódica a la misma del contenido actualizado del Registro de Ficheros de Datos Personales. Asimismo, colaborar con el resto de Registros de Autoridades de Control en la forma en que se determine.

t) En relación al Consejo Consultivo, proponer cuestiones para la emisión de informes y relacionarse con el mismo participando activamente en sus sesiones, de acuerdo a lo que se determine en normas de organización y funcionamiento de aquél.

u) Coordinarse y cooperar con organismos internacionales y órganos de la Unión Europea en materia de protección de datos.

v) Comunicar al Ararteko las actuaciones mencionadas en el artículo 24 de la Ley 2/2004, así como colaborar y coordinarse con el mismo en materia de protección de datos personales.

w) Cualesquiera otras que se le atribuyan en la Ley 2/2004, en el Estatuto de la Agencia Vasca de Protección de Datos, en la presente Resolución y demás disposiciones en vigor, así como todas aquellas funciones de dirección y representación de la Agencia Vasca de Protección de Datos que no estén expresamente atribuidas a otro órgano.

Cuarto.– Unidad de Registro de Protección de Datos y Nuevas Tecnologías. - La Unidad de Registro de Protección de Datos y Nuevas Tecnologías es la unidad administrativa de la Agencia a la que se adscribe el Registro de Protección de Datos previsto en el artículo 18 de la Ley 2/2004 y le corresponde promover la publicidad de la existencia de ficheros de datos de carácter personal que se encuentren dentro del ámbito de aplicación de dicha Ley. Asimismo, y con el objeto de velar por el cumplimiento de la normativa sobre protección de datos de carácter personal, ejercerá la función de inspección sectorial y la coordinación de la red de colaboradores en materia de protección de datos. Por otra parte, tendrá encomendada la realización de estudios relacionados con las nuevas tecnologías y el seguimiento del Plan de Sistemas de la propia Agencia.

Corresponden a la Unidad de Registro de Protección de Datos y Nuevas Tecnologías:

1.– Funciones relacionadas con el Registro de Protección de Datos.

a) Instruir los expedientes de inscripción en el registro de la creación, modificación y cancelación de ficheros a que se refiere el artículo 18.2 de la Ley 2/2004 y demás inscripciones previstas en la ley, así como practicar las notificaciones oportunas al titular del fichero.

b) Recopilar la información contenida en las disposiciones de creación, modificación o cancelación de los ficheros de datos de carácter personal, el contenido de los códigos tipo y las resoluciones relacionadas con el Registro de Protección de Datos.

c) Actualizar y rectificar de oficio los errores materiales de los asientos.

d) Expedir certificaciones de los asientos.

e) Publicar anualmente la relación de los ficheros inscritos, con la información adicional que el Director o Directora de la Agencia Vasca de Protección de Datos determine.

f) Facilitar el acceso de los ciudadanos al Registro de Protección de Datos e informar a las personas que lo soliciten, sobre la existencia o no de ficheros inscritos, su finalidad y la identidad del responsable de los mismos.

g) Preparar y gestionar el envío periódico de las inscripciones realizadas en el Registro de Ficheros de Datos Personales al Registro General de Protección de Datos de la Agencia Española de Protección de Datos.

h) Proponer el dictamen sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos.

2.– Funciones relacionadas con las Inspección.

a) Efectuar inspecciones sectoriales, de conformidad con la planificación de la Agencia, de cualesquiera de los ficheros a que se refiere el artículo 2.1 de la Ley 2/2004, y de los equipos informáticos correspondientes, en los locales que se hallen. A tal efecto podrá realizar las actuaciones contempladas en el artículo 11 del Estatuto de la Agencia Vasca de Protección de Datos.

b) Prestar apoyo a la Unidad de Inspección y Asesoría Jurídica en las tareas de inspección circunstancial en actividades relacionadas con examen de equipos, sistemas de transmisión y acceso de datos, verificación la adecuación del Documento de Seguridad y aquellas otras para las que sea requerida.

3.– Funciones relacionadas con la Red de Colaboradores.

Coordinar la Red de Colaboradores en materia de protección de datos, elaborar y poner a su disposición y a la de los responsables de ficheros, y de sus usuarios, los recursos técnicos para apoyar la inscripción en el Registro de Ficheros de Datos Personales, así como en general la gestión de tales ficheros conforme a lo exigido por la Ley 2/2004 y disposiciones complementarias. Tales recursos podrán incluir, entre otros, metodologías, aplicaciones informáticas de apoyo, esquemas de estandarización de productos o servicios, materiales para la formación, modelos de documentación y guías de preguntas frecuentes.

4.– Funciones relacionadas con las nuevas tecnologías y la gestión de la Agencia.

a) Realizar Estudios sobre el desarrollo y la evolución de las nuevas tecnologías de la información y la comunicación en su relación con la protección de datos personales y asesorar al Director o Directora de la Agencia y al resto de órganos y unidades de la misma en materias de especialización técnica y de gestión relevantes para la protección de datos personales en el ámbito de la sociedad de la información.

b) Desarrollar del plan de sistemas de la Agencia y las directrices de seguridad a utilizar en sus recursos informáticos.

c) Elaborar los informes y propuestas que le solicite el Director o Directora de la Agencia respecto de todas las materias señaladas en los apartados anteriores.

Quinto.– Unidad de Asesoría Jurídica e Inspección. - La Unidad de Asesoría Jurídica e Inspección es la unidad administrativa de la Agencia a la que compete el ejercicio de las funciones derivadas de la potestad de inspección circunstancial y del impulso y la instrucción de los procedimientos a que den lugar las reclamaciones de los ciudadanos para la protección de sus derechos de acceso, rectificación, cancelación y oposición, así como de los procedimientos de infracción de las Administraciones Públicas, Instituciones, Entidades y Corporaciones que se tramiten como consecuencia del ejercicio de la función de control para determinar la existencia o no de infracción prevista en la Ley Orgánica 15/1999, de 13 de diciembre. Igualmente es competencia de esta unidad administrativa la elaboración de informes, la respuesta a consultas y el asesoramiento jurídico de la Agencia Vasca de Protección de Datos.

Corresponden a la Unidad de Asesoría Jurídica e Inspección:

1.– Funciones de Instrucción.

Ejercicio de los actos de instrucción relativos a los procedimientos sancionadores, de tutela de derechos y de infracción por parte de las Administraciones Públicas, Instituciones, Entidades y Corporaciones, derivados del ejercicio de las funciones de control reconocidas a la Agencia.

2.– Funciones de Inspección.

a) Efectuar inspecciones circunstanciales, relacionadas con la instrucción de un expediente, de cualesquiera de los ficheros a que se refiere el artículo 2.1 de la Ley 2/2004, se hallen o no inscritos en el Registro de Protección de Datos, y de los equipos informáticos correspondientes, en los locales que se hallen. A tal efecto podrá realizar las actuaciones contempladas en el artículo 11 del Estatuto de la Agencia Vasca de Protección de Datos.

b) Prestar apoyo a la Unidad de Registro y Nuevas Tecnologías en las tareas de inspección sectorial en actividades relacionadas con el ámbito jurídico y procedimental.

3.– Funciones de Informe, Resolución de Consultas y Asesoría Jurídica.

a) Informar los proyectos de disposiciones que se dicten en desarrollo de la Ley 2/2004.

b) Informar todos aquellos proyectos de disposiciones sobre los que, en relación con la protección de datos personales, le sea solicitado informe.

c) Informar y preparar las respuestas a consultas que sean planteados por las Administraciones Públicas, Instituciones, Entidades y Corporaciones a que se refiere el artículo 2.1 de la Ley 2/2004, y otras personas físicas o jurídicas, con el objeto de elaborar, interpretar y aplicar la legislación en materia de protección de datos.

d) Informar las disposiciones normativas que determinen estadísticas de respuesta obligatoria.

e) Elaborar proyectos de instrucciones y recomendaciones que le solicite el Director o Directora de la Agencia.

f) Asesorar jurídicamente a la Agencia, elaborando los informes y propuestas que le solicite el Director o Directora de la Agencia.

Sexto.– Secretaría General. - La Secretaría General es la Unidad Administrativa responsable del ejercicio de funciones de gestión de recursos humanos y materiales, de gestión económico-administrativa, de otras funciones relacionadas con información general, formación y documentación y de funciones de apoyo y ejecución o instrumentales para el resto de la Agencia.

Corresponden a la Secretaría General:

a) Funciones de Gestión.

a.1.– Gestionar los recursos humanos, ejerciendo la jefatura sobre los mismos.

a.2.– Gestionar los medios materiales de la Agencia.

a.3.– Instruir los procedimientos de provisión ordinarios de concurso de méritos y libre designación de los puestos de trabajo del personal funcionario adscritos a la Agencia, y también las comisiones de servicio cuando afecten a funcionarios de las Administraciones Públicas, Instituciones, Entidades y Corporaciones del artículo 2.1 de la Ley 2/2004.

a.4.– Instruir los procedimientos de selección y promoción profesional del personal laboral adscrito a la Agencia.

a.5.– Instruir los procesos de contratación administrativa.

a.6.– Elaborar, como facultad delegada del Director, el anteproyecto de presupuesto de la Agencia Vasca de Protección de Datos.

a.7.– Realizar la gestión económica-administrativa del presupuesto de la Agencia y, dentro de la misma, como facultad delegada del Director o Directora, aprobar gastos y ordenar pagos, dentro de los límites de los créditos del presupuesto de gastos de la Agencia Vasca de Protección de Datos y conforme a los procedimientos que se establezcan internamente.

a.8.– Llevar el inventario de bienes y derechos que integren el patrimonio de la Agencia.

b) Funciones relacionadas con información general, formación y documentación.

b.1.– Gestionar los fondos documentales de la Agencia, y en particular la creación y actualización de un fondo de documentación sobre legislación, jurisprudencia y doctrina en materia de protección de datos personales y cualesquiera materias conexas.

b.2.– Organizar conferencias, seminarios, jornadas y cualesquiera otras actividades sobre protección de datos.

b.3.– Informar al ciudadano de los derechos que la Ley le reconoce en relación con el tratamiento de sus datos de carácter personal.

c) Funciones de apoyo y ejecución o instrumentales para el resto de la Agencia.

c.1.– Notificar las resoluciones del Director o Directora de la Agencia.

c.2.– Coordinar las relaciones con los medios de comunicación.

c.3.– Preparar Convenios de Colaboración.

c.4.– Gestionar los sistemas de información y telecomunicaciones de la Agencia.

c.5.– Ejercer, de acuerdo con sus normas de organización y funcionamiento, la Secretaría del Consejo Consultivo.

c.6.– Coordinar las prácticas universitarias realizadas en el Agencia con los alumnos de aquellas Universidades con las que se suscriba Convenio de colaboración.

c.7.– Gestionar los asuntos de carácter general no atribuidos a otros órganos de la Agencia.

c.8.– Elaborar los informes y propuestas que le solicite el Director o Directora de la Agencia respecto de todas las materias señaladas en los apartados anteriores.

Séptimo.– Dependencias. Funcionamiento horizontal. - Las tres unidades dependerán jerárquicamente del Director o Directora y tendrán la responsabilidad sobre las áreas mencionadas. Ahora bien, sus responsables y el personal que se asigne a cada una de las unidades deberán realizar actividades para las otras en la medida en que se determine en el plan de gestión o de actuación específicos para un periodo temporal o cuando así lo determine el Director o Directora.

Octavo.– Órganos colegiados. El Consejo Consultivo. - El Consejo Consultivo de Protección de Datos, previsto en el artículo 14 de la Ley 2/2004, es el órgano colegiado de asesoramiento al Director o Directora de la Agencia Vasca de Protección de Datos, tiene atribuidas las funciones que le atribuyen la Ley 2/2004 y el Estatuto de la Agencia Vasca de Protección de Datos y se regirá por sus propias normas de organización y funcionamiento.

Noveno.– Régimen de sustituciones. - En los casos de vacante, ausencia o enfermedad de los titulares de las Unidades, las funciones atribuidas a los mismos serán ejercidas, mientras dure tal situación por la persona que determine el Director o Directora.

Décimo.– Eficacia. - La presente Resolución será de aplicación a partir del día siguiente a su publicación en el Boletín Oficial del País Vasco.