Osakidetza

LEGISLACIÓN Y NORMATIVA E INSTRUCCIONES EN MATERIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Septiembre 2007

Osakidetza

PROTECCIÓN DE DATOS

LEGISLACIÓN

LEGISLACIÓN ESPECIFICA EN MATERIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

- ✓ Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- ✓ 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.

- ✓ 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.

- ✓ Ley 41/2002, de 14 de diciembre, Básica reguladora de la autonomia del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Osakidetza

NORMATIVA APLICABLE

NORMATIVA E INSTRUCCIONES EMITIDAS POR OSAKIDETZA-SVS EN MATERIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

- ✓ ACUERDO de 19 de junio de 2006, del Consejo de Administración del Ente Público Osakidetza-Servicio vasco de salud, por el que se regulan los ficheros de carácter personal gestionados por Osakidetza-Servicio vasco de salud.

- ✓ ACUERDO de 24 de enero de 2007, del Consejo de Administración de Osakidetza-Servicio vasco de salud, por el que se modifica la estructura de la Comisión de Seguridad para la Protección de Datos de Osakidetza-Servicio vasco de salud.

- ✓ Instrucción Nº 2/2003 - Dirección General. Asunto : Modelo organizativo de seguridad para las organizaciones de servicios de Osakidetza/SVS.

- ✓ ACUERDO de 28 de marzo de 2003, del Consejo de Administración de Osakidetza-Servicio vasco de salud, por el que se crea y se asignan funciones a la Comisión de Seguridad para la Protección de Datos de Osakidetza-Servicio vasco de salud.

- ✓ Instrucción Nº 6/2003 - Dirección General. Asunto : Funciones y obligaciones del personal de Osakidetza/SVS, con relación a la protección de datos de carácter personal. Procedimiento de actuación.

Osakidetza

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal

Septiembre 2007

LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

(Cambio denominación por artículo 79 Ley 62/2003, de 30 de noviembre: Las referencias a la Agencia de Protección de Datos deberán entenderse realizadas a la Agencia Española de Protección de Datos).

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto

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

Artículo 2. Ámbito de aplicación

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

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

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.
c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

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

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

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

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

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

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

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

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

Artículo 3. Definiciones

A los efectos de la presente Ley Orgánica se entenderá por

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

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

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

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

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

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

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

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

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

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

TÍTULO II

PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Artículo 4. Calidad de los datos

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

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

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

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por

los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artículo 6. Consentimiento del afectado

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

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

datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

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

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

Artículo 7. Datos especialmente protegidos

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

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

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

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

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

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

6. No obstante lo dispuesto en los apartados anteriores podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los

apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

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

Artículo 8. Datos relativos a la salud

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

Artículo 9. Seguridad de los datos

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

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

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

Artículo 10. Deber de secreto

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que

subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11. Comunicación de datos

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

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

a) Cuando la cesión está autorizada en una Ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

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

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

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

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

Artículo 12. Acceso a los datos por cuenta de terceros

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

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

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

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

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

TÍTULO III

DERECHOS DE LAS PERSONAS

Artículo 13. Impugnación de valoraciones

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

2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único

fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

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

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

Artículo 14. Derecho de Consulta al Registro General de Protección de Datos

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

Artículo 15. Derecho de acceso

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

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

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

Artículo 16. Derecho de rectificación y cancelación

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

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

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

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

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

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

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

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

Artículo 18. Tutela de los derechos

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

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

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

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

Artículo 19. Derecho a indemnización

1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento,

sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

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

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

TÍTULO IV

DISPOSICIONES SECTORIALES

CAPÍTULO PRIMERO

Ficheros de titularidad pública

Artículo 20. Creación, modificación o supresión

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

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

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

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

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

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

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

f) Los órganos de las Administraciones responsables del fichero.

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

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

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

Artículo 21. Comunicación de datos entre Administraciones Públicas

1. Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. *(Resultado STS 292/2000, de 30 de noviembre)*

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

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

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

Artículo 22. Ficheros de las Fuerzas y Cuerpos de Seguridad

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

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

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

pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

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

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

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

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

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

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

Artículo 24. Otras excepciones a los derechos de los afectados

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales. *(Resultado STS 292/2000, de 30 de noviembre)*

CAPÍTULO II

Ficheros de titularidad privada

Artículo 25. Creación

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

Artículo 26. Notificación e inscripción registral

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

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

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

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

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

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

Artículo 27. Comunicación de la cesión de datos

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

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

Artículo 28. Datos incluidos en las fuentes de acceso público

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

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

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

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

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

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

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

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

1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público

establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

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

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

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

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

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

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

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

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

Artículo 31. Censo Promocional

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

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

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

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

Artículo 32. Códigos tipo

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

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

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

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

la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

TÍTULO V

MOVIMIENTO INTERNACIONAL DE DATOS

Artículo 33. Norma general

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

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

Artículo 34. Excepciones

Lo dispuesto en el artículo anterior no será de aplicación:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

TÍTULO VI

AGENCIA DE PROTECCIÓN DE DATOS

Artículo 35. Naturaleza y régimen jurídico.

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

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

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

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

a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.

b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.

c) Cualesquiera otros que legalmente puedan serle atribuidos.

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

Artículo 36. El Director

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

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

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

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

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

Artículo 37. Funciones

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 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 82.1 Ley 62/2003, de 30 de diciembre)*

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 de Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

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

4. Son infracciones muy graves:

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

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

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

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

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

f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando

con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

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

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

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

Artículo 45. Tipo de sanciones

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

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

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

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

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

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

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

Artículo 46. Infracciones de las Administraciones Públicas

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

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

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

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

Artículo 47. Prescripción

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

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

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

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

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

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

Artículo 48. Procedimiento sancionador

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

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

3. Los procedimientos sancionadores tramitados por la Agencia 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 82.2 Ley 62/2003, de 30 de diciembre)*

Artículo 49. Potestad de inmovilización de ficheros

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

DISPOSICIONES ADICIONALES

Primera. Ficheros preexistentes

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

En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica y la obligación prevista en el párrafo anterior deberá cumplimentarse en el plazo de doce años a contar desde el 24

de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

Segunda. Ficheros y Registro de Población de las Administraciones Públicas.

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

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

Tercera. Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social.

Los expedientes específicamente instruidos al amparo de las derogadas Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social, que contengan datos de cualquier índole susceptibles de afectar a la seguridad, al honor, a la intimidad o a la imagen de las personas, no podrán ser consultados sin que medie consentimiento expreso de los afectados, o hayan transcurrido 50 años desde la fecha de aquéllos.

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

Cuarta. Modificación del artículo 112.4 de la Ley General Tributaria.

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

4. La cesión de aquellos datos de carácter personal, objeto de tratamiento que se debe efectuar a la Administración tributaria conforme a lo dispuesto en el artículo 111, en los apartados anteriores de este artículo o en

otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito tampoco será de aplicación lo que respecto a las Administraciones Públicas establece el apartado 1 del artículo 21 de la Ley Orgánica de Protección de Datos de carácter personal.

Quinta . Competencias del Defensor del Pueblo y órganos autonómicos semejantes.

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

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

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

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

También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.

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

DISPOSICIONES TRANSITORIAS

Primera. Tratamientos creados por Convenios Internacionales

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

Segunda. Utilización del Censo Promocional

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

Tercera. Subsistencia de normas preexistentes.

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

DISPOSICIÓN DEROGATORIA

Única

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

DISPOSICIONES FINALES

Primera. Habilitación para el desarrollo reglamentario

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

Segunda. Preceptos con carácter de Ley Ordinaria

Los títulos IV, VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la Disposición Adicional Cuarta, la Disposición Transitoria Primera y la Final Primera, tienen el carácter de Ley Ordinaria.

Tercera. Entrada en vigor

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

Palacio del Congreso de los Diputados, a 25 de noviembre de 1999.

Federico Trillo-Figueroa Martínez-Conde
PRESIDENTE DEL CONGRESO DE LOS DIPUTADOS

Osakidetza

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

Septiembre 2007

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.

CAPÍTULO I.- DISPOSICIONES GENERALES

Artículo 1.- Ámbito de aplicación y fines.

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

Artículo 2.- Definiciones.

A efectos de este Reglamento, se entenderá por:

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

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

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

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

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

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

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

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

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

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

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

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

Artículo 3.- Niveles de seguridad.

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

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

Artículo 4.- Aplicación de los niveles de seguridad.

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

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

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

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

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

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

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

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

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

Artículo 7.- Ficheros temporales.

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

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

CAPÍTULO II.- MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 8.- Documento de seguridad.

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

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

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

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

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

Artículo 9.- Funciones y obligaciones del personal.

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

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

Artículo 10.- Registro de incidencias.

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

Artículo 11.- Identificación y autenticación.

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

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

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

Artículo 12.- Control de acceso.

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

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

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

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

Artículo 13.- Gestión de soportes.

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

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

Artículo 14. - Copias de respaldo y recuperación.

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

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

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

CAPÍTULO III.- MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 15.- Documento de seguridad.

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

Artículo 16.- Responsable de seguridad.

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

Artículo 17.- Auditoría.

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

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

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

Artículo 18.- Identificación y autenticación.

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

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

Artículo 19.- Control de acceso físico.

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

Artículo 20.- Gestión de soportes.

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

2.- Igualmente, se dispondrá de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes,

el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

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

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

Artículo 21.- Registro de incidencias.

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

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

Artículo 22.- Pruebas con datos reales.

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

CAPÍTULO IV.- MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Artículo 23.- Distribución de soportes.

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

Artículo 24.- Registro de accesos.

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

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

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

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

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

Artículo 25.- Copias de respaldo y recuperación.

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

Artículo 26.- Telecomunicaciones.

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

CAPÍTULO V.- INFRACCIONES Y SANCIONES.

Artículo 27.- Infracciones y sanciones.

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

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

2.- Cuando se trate de ficheros de los que sean responsables las Administraciones Públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 45 de la Ley Orgánica 5/1992.

Artículo 28.- Responsables.

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

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

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

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

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

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

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

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

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

Orden de 31-7-1998 del Ministerio de Justicia por la que se amplía la relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos.

Osakidetza

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

Septiembre 2007

Xedapen Orokorrak

LEHENDAKARITZA

Zk-1184

2/2004 LEGEA, otsailaren 25ekoa, Datu Pertsonaletarako Jabetza Publikoko Fitxategiei eta Datuak Babesteko Euskal Bulegoa Sortzeari buruzkoa.

Eusko Legebiltzarrak otsailaren 25ko 2/2004 Legea, Datu Pertsonaletarako Jabetza Publikoko Fitxategiei eta Datuak Babesteko Euskal Bulegoa Sortzeari buruzkoa, onartu duela jakinarazten zaie Euskadiko herritar guztiei.

OTSAILAREN 25EKO 2/2004 LEGEA, DATU PERTSONALETARAKO JABETZA PUBLIKOKO FITXATEGIEI ETA DATUAK BABESTEKO EUSKAL BULEGOA SORTZEARI BURUZKOA

ZIOEN ADIERAZPENA

Teknikaren aurrerabidea bizkortu egin da azken aldi honetan. Gaur egun, informatika erabiliz, pertsona fisikoei buruzko hainbat eta hainbat datu trata dezakegu, eta baliteke intimitatea urratzen duen hainbat gauza ezagutzea pertsona horiei buruz. Baliteke teknologiak eskaintzen dizkigun aukerak maltzurkeriaz erabiltzea baten batek, bakoitzaren intimitaterako gorde beharreko esparruen kaltetan, eta ordenamendu juridikoek ezin dute ezikusia egin.

Teknologiaren, batez ere informatikaren, eta pertsonen intimitatearen arteko tentsio horrek legearen eskuhartzea eskatzen du, bi ondasun horien artean oreka asegarria lortzeko, biak baitira legez babestea merezi dutenak. Alde batetik, garapen teknologikoari galga emateak ez dio gizarteari onik egiten, teknologiak aukera mugagabeak eskaintzen baititu, gizartearen ongizatea hobetu behar dutenak; baina, beste alde batetik, herritarrek beren intimitate pertsonala babesturik ikusteko eskubidea dute, eta gaur egungo teknologia informatikoak eskaintzen dituen aukerek ez dute intimitate hori nahi baino gehiago murriztu behar. Horretarako, informatika erabiltzeari mugak jarri behar, eta, horrela, herritarrei ohorea eta intimitatea, pertsonala eta etxekoa, eta eskubideen bete-beteko erabilera bermatu. Konstituzioak hala egiteko agintzen dio legegileari, 18.4 artikuluan, eta hark agindu hori jaso egin du Datu Pertsonalak Babesteko abenduaren 13ko 15/1999 Lege Organikoan.

Herritarren intimitate pertsonala eta etxeko intimitatea babesteko kezka horrek –informatika halakoetan

Disposiciones Generales

PRESIDENCIA DEL GOBIERNO

Nº-1184

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 hace saber a todos los ciudadanos y ciudadanas de Euskadi que el Parlamento Vasco ha aprobado la siguiente Ley:

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.

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 consiguien-

noiz-nola erabili mugatu behar horretarako– ez da Estatuko legegilearen kontua soilik. Europar Batasuneko erakundeek ere badakite zer den hori, eta halaxe adierazi izan dute.

Europako Erkidegoa eratzeko itunak gaur egun daukan 286. artikulua Amsterdamgo Itunak ekarria da (1997ko ekainaren 17koa da Amsterdamgo itun hori), eta, hor agindurik dagoenez, datu pertsonalen tratamendua edo zirkulazio askea dela-eta pertsonak babestearren ezer erabakitzen badu Batasunak, Batasuneko erakundeek eta organismoek ere bete behar dituzte erabaki horiek.

Lehenagotik ere, Europako Legebiltzarrak eta Kontseiluak emana zuten 1995eko urriaren 24ko 95/46/EE Zuzentaraua, datu pertsonalen tratamendua eta zirkulazio askea dela-eta pertsona fisikoak babesteari buruzkoa. Eta, printzipio modura, zuzentarau horretan jasota dago datuak tratatzeko sistemak gizon-emakumeon zerbitzura daudela, eta derrigor zaindu behar dituztela pertsona fisikoen oinarrizko askatasunak eta eskubideak, intimitatea batez ere, eta ekonomia eta gizartea garatzen, elkartrukeak garatzen eta norbanakoon ongizatea areagotzen lagundu behar dutela.

Zuzentarau horren arabera, estatuek datu pertsonalen tratamenduari buruz dituzten legeek eskubide eta askatasun horien errespetua bermatzea dute helburu, bizitza pribatua errespetatzeko eskubidea bereziki, hala aitorturik baitago Giza Eskubideak eta Oinarrizko Askatasunak Babesteko Europako Hitzarmeneko 8. artikuluan eta Batasuneko zuzenbideko printzipio orokorretan, eta, legedi horiek bata bestera hurbiltzekotan, kontu horiei babes handia emateko izan behar du.

Zuzentarau horren arabera –eta datu pertsonalak babesteaz ari gara orain–, kontroleko aginte bat sortzea da pertsonek behar duten babesaren funtsezko osagai bat. Batasuneko estatu bakoitzean aritu beharko du aginte horrek, inongo loturarik gabe, eta bere lana egiteko behar dituen baliabide guztiak izan beharko ditu, berdin dio zer edo zer ikertzeko izan edo inon esku hartzeko izan.

Zuzentarau horretan jasota dagoenez, Batasuneko estatuek hiru urteko epea dute zuzentaraua betetzeko beharrezko xedapenak emateko, dela legez, dela erregelamenduz edo dela administrazio-mailan.

Datuak babestearren Batasuneko erakundeak ez dira, besterik gabe, erkidegoko estatuetarako zuzentarausail bat sortzera mugatu. Datu pertsonalen tratamenduari dagokionez, Batasuneko erakundeetan ere, pertsona fisikoak babesteko hainbat neurri hartu dute. Horretarako onartu zuten Europako Legebiltzarrak eta Kontseiluak, 2000.eko abenduaren 18an, 45/2001 (EE) Erregelamendua, eta kontroleko aginte aske bat ere sortu zuen erregelamendu horrek (Datuak Babesteko Ikuskatzaile Europarra).

te 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 Amsterdam 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 disponer 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) N.º 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).

Itxura denez, datu pertsonalak eta intimitatea ondo babestu beharra bide-argi moduko bat da Batasunaren arauetarako, eta justu datu pertsonalen babesa arautzeko ez diren beste zuzentarau-proposamen batzuk ere hartzen ditu itzalpean behar horrek, hala nola komunikazio elektronikoetarako sare eta zerbitzuak arautzeko esparru erkide bati buruz Europako Legebiltzarrak eta Kontseiluak egin zuten zuzentarau-proposamena (Aldizkari Ofiziala, C 365 E , 2000/12/19koa).

Barruko zuzenbidean, berriz –lehenago ere esan dugu–, datu pertsonalak babesteko lege organikoan dago arauturik datu pertsonalen babesa (15/1999 Lege Organikoan, abenduaren 13koan). Lege horretan daude arauturik Datuak Babesteko Bulegoaren araubide juridikoaren oinarrizko alderdiak, Konstituzioko 18.4 artikuluan aipaturiko oinarrizko eskubidearekin zerikusia duten beste gai batzuekin batera. Bulego horrek beteko du 95/46/EE Zuzentarauan aipaturiko kontrol-aginte askearen lana.

Lege organiko horretan agindurik dagoenez, autonomia-erkidegoek edo erkidego horietako tokiko administrazioek datu pertsonaletarako sorturiko edo kudeaturiko fitxategiekin baldin badute zerikusia bulego horretako zereginek, erkidego bakoitzeko organoek beteko dituzte eginkizun horietako gehienak. Halakoetan, organo horiek izango dira kontroleko aginteak, eta lanerako erabateko objektibitatea eta independentzia bermatu behar zaie. Legezko irizpide hori 95/46/EE Zuzentarauko 28. artikuluarekin bat dator; artikulu horretan jartzen duenez, Batasuneko estatuek, zuzentarau horren itzalpean hartzen dituzten xedapenak betetzen ote diren zaintzearren beren lurraldean, aginte publiko bat edo gehiago izango dute hartara jarria; eta beste gauza bat ere gehitzen du: aginte horiek inongo loturarik gabe beteko dituztela agintzen dizkieten eginkizunak.

Eta nola antolaturik dagoen bada kontua, legeak hiru titulu ditu:

I. tituluan xedapen orokorrak jaso ditugu. Hor daude zehazturik legearen xedea eta aplikazio-eremua, eta hor dago zedarriturik zein fitxategi geratu den legearen araupean, sortu dituen edo kudeatzen dituen herri-administrazio, erakunde edo korporazioaren arabera. Zedarritze hori osatze aldera, legea zein fitxategitan ez den aplikatuko eta, araubide bereziren bat dutela-eta, zeinetan aplikatuko den ere zehazten da. Definizio-zerrenda bat ere badakar, erabilgarria oso, arautu dugun gai honetako terminologia berezia zehaztu eta bateratzeko; beste hainbat konturen inguruko hainbeste alderdi ere badakar arauturik, esate baterako fitxategiak sortzea, aldatzea edo ezabatzea, datu pertsonalak biltzeko mugak, interesdunentzako informazioa, datu-fitxategien segurtasuna, bai eta Datuak Babesteko Euskal Bulegoan erreklamazioak nola jarri ere. Titulu beharrezkoa, inondik ere, legeari koherentzia sistematikoa eta osotasuna emateko, gero garatu egin beharko dena.

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 n.° 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.

II. tituluan, berriz, Datuak Babesteko Euskal Bulegoa sortu, eta hango araubide juridikoaren funtsezko alderdiak arautu ditugu. Bertako langileen erregimena dela, baliabide ekonomikoak direla, aurrekontu-sistema dela, gobernu-organoak direla, eginkizunak direla edo aginpideak direla, horri denari buruzko hainbat agindu dakar. Datuak Babesteko Erregistroaren sorrera dakarrela ere aipatu behar, bulegoak bai baitu haren beharra.

Zehatzeko araubiderako utzi dugu III. titulua. Erantzuleak nor diren, arau-hausteen tipifikazioa eta dagozkien zigorrak datoz jasota. 45/2001 (EE) Erregelamenduan jartzen duenez –lehen ere aipatu dugu–, datu pertsonalak babesteko sistemak ezinbestekoa du eskubide-betebeharrak zehaztea, baina baita arau-hausleentzako modu-moduko zigorrak ere. Gure honetan, berriz, fitxategien titularrak nor diren ikusita, titular bereziak baitira, administrazio, erakunde eta korporazioetako langileen arau-hausteak hartu ditugu, batez ere, kontuan, halakoen fitxategietan aplikatu behar denez legea.

Lege honek hiru xedapen gehigarri ditu. Fitxategien berri Datuak Babesteko Euskal Bulegoari eman beharraz da bat; Autonomia Administrazioak eta foru-administrazioek, beren aginpideak betetze aldera, udalerrolda nola erabili behar duten dakar bigarrenak; eta Arartekoaren eta Datuak Babesteko Estatuko Bulegoaren aginpideak babestu beharraz da hirugarrena.

Amaitzeko, azken xedapenean, legea garatzeko eta aplikatzeko baimena ematen zaio Eusko Jaurlaritzari.

I. TITULUA

XEDAPEN OROKORRAK

1. artikulua.– Xedea

Hauxe da lege honen xedea:

1.– Euskal Autonomia Erkidegoak, lurralde historikoetako foru-erakundeek eta Euskal Autonomia Erkidegoko toki-erakundeek datu pertsonaletarako sorturiko edo kudeaturiko fitxategiak arautzea.

2.– Datuak Babesteko Euskal Bulegoa sortzea eta arautzea.

2. artikulua.– Aplikazio-eremua

1.– Datu pertsonaletarako fitxategietan aplika daiteke lege hau. Zuzenbide publikoko ahalak gauzatzeko sortu edo kudeatuak behar dute izan fitxategi horiek; honako hauek sortuak edo kudeatuak:

a) Autonomia Erkidegoko Administrazio orokorrak, lurralde historikoetako foru-organoek, Euskal Autonomia Erkidego barruko toki-administrazioek eta, zuzenbide publikoko ahalak gauzatzeko sortu bazituzten, herri-administrazioen menpeko edo haietara loturiko edonolako erakunde publikoek.

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) N.º 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) Eusko Legebiltzarrak.

c) Herri Kontuen Euskal Epaitegiak.

d) Arartekoak.

e) Lan Harremanen Kontseiluak.

f) Ekonomia eta Gizarte Arazoetarako Batzordeak.

g) Kooperatiben Goren Kontseiluak.

h) Datuak Babesteko Euskal Bulegoak.

i) Ebazpen Batzordeak.

j) Interes ekonomiko eta profesionalak ordezkatzen dituzten Euskal Autonomia Erkidegoko zuzenbide publikoko korporazioek.

k) Eusko Legebiltzarrak lege bidez sorturiko beste edozein organismo edo erakundek –berdin dio nortasun jurdikoa duen edo ez–, lege horrek bestelakorik xedatzen ez badu.

2.– Aurreko zenbaki horretan jarrita dagoena jarrita dagoela ere, honako fitxategi hauetan ez da aplikatuko lege hau:

a) Sekretutzat jotako gaietarako babes-arauen pean dauden fitxategietan.

b) Terrorismoa eta delinkuentzia-modu antolatu latriak ikertzeko dauden fitxategietan.

c) Hauteskunde-araubideko legeek arauturikoetan.

d) Euskadiko poliziek bideokamera bidez lorturiko irudi eta hotsetatik sorturiko fitxategietan, gai horri buruzko legeen arabera.

3.– Estatistiketarako besterik ez badira eta funtzio estatistiko publikoari buruzko legeen babesean badaude, datu pertsonalak tratatzeko, hartarako berariazko xedapenak eta –halako ezer xedatzen badu– lege honetan bereziki xedaturikoa bete beharko dira.

4.– Osasuneko erakunde eta zentro publikoek eta hor lan egiten duten profesionalek osasun-arloko legeetan xedaturik dagoenaren arabera tratatu ahal izango dituzte etortzen zaizkien gaixoen edo bertan tratatu behar dituzten gaixoen osasunari buruzko datu pertsonalak. Hala ere, lege horiekin bateraezina ez den guztirako, lege honetan xedaturikoa ere bete beharko da.

5.– Euskadiko poliziek datu pertsonaletarako sortu edo kudeatzen dituzten fitxategietan ere –artikulu honetako 2. zenbakian agertzen direnen artean ez badaude– lege honetan xedaturikoa aplikatu beharko da, araubide juridikoan dituzten berezitasunak zainduta. Hemen daude berezitasun horiek: Datu Pertsonalak Babesteko abenduaren 13ko 15/1999 Lege Organikoan eta Euskal Autonomia Erkidegoko Poliziari buruzko uztailaren 17ko 4/1992 Legean.

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 personas 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.

3. artikulua.– Definizioak

Lege honen ondorioetarako, hona hemen definizio batzuk:

a) Datu pertsonalak: identifikatutako edo identifika daitezkeen pertsona fisikoen gaineko edozein informazio. Zuzenean edo zeharka nor den jakiteko moduko edonor da identifikagarria, eta, bereziki, nortasunzenbaki baten bidez edo ezaugarri baten edo batzuen bidez identifika daitekeen edonor, berdin dio ezaugarri horiek fisikoak, fisiologikoak, psikikoak, ekonomikoak, kulturakoak edo sozialak izan.

b) Fitxategia: datu pertsonalen multzo antolatu oro, datu-multzoa sortu, jaso, antolatu eta eskuratzeko modua edozein dela ere.

c) Datuen tratamendua: eragiketa eta prozedura teknikoak dira –batzuetan automatizatuak beste batzuetan ez–, eta datuak bildu, grabatu, gorde, landu, aldatu, blokeatu eta indarrik gabe uzteko aukera ematen dute. Komunikazio, kontsulta, elkarkonexio eta transferentzien eraginez datuak uztea ere datuak tratatzea da.

d) Fitxategiaren edo tratamenduaren erantzulea: pertsona, erakunde, entitate, korporazio edo administrazio-organoren bat izango da, hari atxikita egongo da fitxategia, eta hark erabakiko du tratamendua zertarako den, zein eduki duen eta nola egin behar den. Fitxategia sortzen duen xedapenean zehaztuko da nor den erantzulea. Segurtasuneko agirian zehazturikoak izango dira erantzulearen eginkizunak.

e) Tartekoa edo interesduna: tratatu beharreko datuen titularra den pertsona fisikoa. Artikulu honetako c) letran dago zehazturik tratatze hori.

f) Tratamenduaren arduraduna: pertsona fisikoa edo juridikoa, aginte publikoa, zerbitzua edo beste edozein erakunde izan daiteke, eta hark tratatzen ditu, arduradunaren aginduz, berak bakarrik edo beste batzuekin batera, datu pertsonalak.

g) Interesdunaren adostasuna: interesdunak baiezkoa ematea bere datu pertsonalak tratatzeari; inork inola estutu gabe, zalantzarako biderik eman gabe, berariaz eta zer egiten duen jakinda egin beharko du.

h) Datuak uztea edo jakinaraztea: interesduna ez den beste pertsona bati datuak erakustea.

4. artikulua.– Fitxategiak sortzea, aldatzea eta ezabatzea

1.– Autonomia Erkidegoko Administrazioko fitxategiak sortzeko, aldatzeko eta ezabatzeko, dena delako fitxategia atxikita dagoen saileko titularraren agindu bidez egin beharko da. Indarrean dauden legeek eskatutako aipamen guztiak jaso beharko ditu agindu horrek, eta Euskal Herriko Agintaritzaren Aldizkarian argitaratu beharko da. Agindu hori egiteko prozedura xedapen orokorrak egiteko erabakita dagoen berbera izango da.

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.– Datu pertsonalen fitxategiak beste administrazio, erakunde edo korporazio batzuetakoak badira, berriz, hura sortu, aldatu edo ezabatzeko erabakiak edo xedapenak derrigorrezko aipamen guztiak jaso beharko ditu eta Euskal Herriko Agintaritzaren Aldizkarian edo lurralde historikoko aldizkarian argitaratuko da, fitxategia duenaren eginkizun edo aginpideak zein lurralde-eremutara iristen diren kontuan hartuta.

5. artikulua.– Datu pertsonalak biltzea

Lege honetako 2.1 artikuluan aipaturik dauden herri-administrazioek eta gainerako erakunde, korporazio eta entitateek beren aginpideak gauzatzeko egokiak, beharrezkoak eta neurrikoak dituztenean baino ezin ditzakete bildu, tratatzeko asmoz, datu pertsonalak. Legez bestelakorik agintzen ez bada behinik behin, datu horiek biltzeko ez da tartean direnen adostasuna eskatu behar, baina biltzerakoan datu horiek zituzten helburu jakin, zehatz eta zilegietarako bakarrik erabili behar dituzte, nahiz eta gero helburu historiko, estatistiko edo zientifikoetarako erabil daitezkeen, aplikatu beharreko legeen arabera.

6. artikulua.– Interesdunei eman beharreko informazioa

Interesdunei datu pertsonalik eskatzera, jakin beharrekoak azaldu behar zaizkie aurretiaz, halako datuak babesteko legeen arabera. Baina datu horiek ez badituzte interesdunarengandik berarengandik jaso, eta ezinezkoa bada hari informazioa ematea edo informazioa emate horrek neurrigabeko ahaleginak egin beharra eskatzen badu interesdunak asko direlako, datuak zaharrak direlako edo ordaina eman beharra legokeelako, halakoetan Datuak Babesteko Euskal Bulegoko zuzendariak, aipatutako legeekin bat eginik, fitxategiaren erantzulea interesdunei informazioa eman behar horretatik libre utz daiteke.

7. artikulua.– Segurtasuneko agiriaren gutxieneko edukia onartzea

Lege honetako 2.1 artikuluan aipaturik dauden herri-administrazioetako, erakundeetako eta korporazioetako gobernu-organoek, beren buruak antolatzeko ahalmenaz baliatuz, segurtasuneko agiriaren gutxieneko edukia onar dezakete, datuen segurtasunari buruzko aginduak betetzearren eta dena delako administrazio, erakunde edo korporazio hori titular duten fitxategi guztietan edo fitxategi horietako batzuetan aplikatzeko asmoz. Edonola ere, segurtasuneko agiri hori fitxategiko arduradunek egin eta ezarri behar dute, fitxategi horietako datu pertsonalen segurtasuna bermatzeko.

8. artikulua.– Interesduenen eskubideak erabiltzeko prozedura

1.– Datuen aurka egiteko, datuetara iristeko, datu horiek zuzentzeko, indarrik gabe uzteko eta legeak onarturiko beste edozertarako eskubidea izango dute interesdunek. Legean zehazturikoa izango da eskubide horien edukia.

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

En el 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.– Los 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.– Aurreko zenbakian zehazturiko eskubideak erabiltzeko prozedura administrazio, erakunde edo korporazio bakoitzak arautuko du, erregelamendu bidez, lege hau bete behar duten beren fitxategietarako. Horregatik ez dute inolako ordainik eskatuko.

9. artikulua.– Datuak Babesteko Euskal Bulegoan erreklamazioak aurkeztea

1.– Lege honetan xedaturikoaren aurka ezer egiten badu inork, interesdunek Datuak Babesteko Euskal Bulegoan erreklama dezakete. Erregelamendu bidez zehaztuko da nola.

2.– Interesdunen bati ez badiote uzten datuen aurka egiteko, datuetara iristeko, datuak zuzentzeko, indarrik gabe uzteko edo legeetan –datu pertsonalak babesteko legeetan– aitorturiko beste edozertarako eskubidea erabiltzen, Datuak Babesteko Euskal Bulegoari jakinarazteko aukera izango du, eta hark, orduan, ezezko hori bidezkoa den edo ez ikusi beharko du.

3.– Gehienez ere sei hilabeteko epea dago eskubideak ziurtatzeko berariazko ebazpena emateko eta jakinarazteko, eta administrazio-isiltasunak, halakoetan, eskatutako ziurtatze horri ezezkoa eman diotela esan nahiko du.

4.– Administrazioarekiko auzi-errekurtsoa jar daiteke Datuak Babesteko Euskal Bulegoaren ebazpenen aurka. Nahi izanez gero, aurretiaz, berraztertzeko errekurtsoa jar daiteke.

II. TITULUA

DATUAK BABESTEKO EUSKAL BULEGOA

10. artikulua.– Sorrera eta araubide juridikoa

1.– Datuak Babesteko Euskal Bulegoa sortzen da. Zuzenbide publikoko entea izango da, nortasun juridiko propioa eta gaitasun publiko eta pribatu erabatekoa izango ditu, eta herri-administrazioekiko inongo loturarik gabe beteko ditu bere eginkizunak. Lege honetan eta bere estatutuan xedatutakoaren arabera jardungo du; estatutu hori Eusko Jaurlaritzaren dekretu baten bidez onartu beharko da, Lehendakariordetzak proposaturik.

2.– Administrazioaren ahalak gauzatu behar dituenean, Datuak Babesteko Euskal Bulegoak azaroaren 26ko 30/1992 Legea bete beharko du, Herri Administrazioen Araubide Juridikoaren eta Administrazio Prozedura Erkidearen Legea. Gainerako jardunean, Datu Pertsonalak Babesteko abenduaren 13ko 15/1999 Lege Organikoa, lege hau eta lege horiek garatzeko xedapenak bete beharko ditu.

3.– Ondarerik eskuratzeko edo ezer kontratatzeko, indarrean dagoen zuzenbide publikoa bete beharko du Datuak Babesteko Euskal Bulegoak. Bulegoaren ondasun eta eskubideak Euskal Autonomia Erkidegoaren ondarekoak izango dira.

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.– Las 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.– Auzibidean jardun beharra badago, Euskal Autonomia Erkidegoko Administrazioko zerbitzu juridikoen ardura izango da Datuak Babesteko Euskal Bulegoa ordezkatzea eta defendatzea, arauetan xedaturik daukatenaren arabera.

11. artikulua.– Langileak

1.– Lege honetako 2.1 artikuluan aipaturik datozen herri-administrazioetako eta erakundeetako funtzionarioek eta propio kontrataturiko langileek beteko dituzte Datuak Babesteko Euskal Bulegoko lanpostuak, lanpostu bakoitzak dituen eginkizunen arabera. Beren lanean ezagutzen dituzten datu pertsonalak isilpean gorde beharko dituzte langile horiek, derrigor.

2.– Datuak Babesteko Euskal Bulegoko langileak Euskal Autonomia Erkidegoko Administrazio orokorreko funtzio publikoko arauen pean egongo dira. Arau horiekin bat, Datuak Babesteko Euskal Bulegoari dagokio lanpostuak eskuratzeko sistema erabakitzea, baldintzak eta hautaproben ezaugarriak zehaztea, bai eta lanpostuak betetzeko eta laneko sustapeneko prozeduretako deialdiak egitea eta prozedura horiek kudeatzea eta ebaztea ere.

3.– Ahal publikoak erabili beharra daukaten lanpostuak funtzionarioentzat gordeta egongo dira.

12. artikulua.– Baliabideak

Datuak Babesteko Euskal Bulegoak honako ondasun eta baliabide hauek izango ditu bere eginkizuna betetzeko:

a) Autonomia Erkidegoko Aurrenkontu Orokorretan urtero izendatuko zaion diru-kopurua.

b) Ematen dizkioten diru-laguntzak eta egiten dizkioten ekarpenak.

c) Bere jardunak ematen dizkion diru-sarrerak, ohikoak nahiz ohiz kanpokoak.

d) Ondarekoak dituen ondasunak eta baloreak, eta haiek ematen dituzten produktu eta errentak.

e) Legez ematen dioten beste edozein ondasun edo baliabide.

13. artikulua.– Aurrekontua

Datuak Babesteko Euskal Bulegoak urtero-urtero aurrekontu-aurregitasmoa egin eta onartu beharko du. Gero, Eusko Jaurlaritzara bidali beharko du, han, behar bezain ondo bereizita, Autonomia Erkidegoko Aurrekontu Orokorretan sar dezaten, Euskal Autonomia Erkidegoko aurrekontu-sistema arautzen duten legeen arabera. Lege horiek bete beharko ditu bere aurrekontua aldatzeko, gauzatzeko eta kitatzeko araubideari dagokionez. Horretarako, kontuan hartu beharko du erakundearen izaera, kontabilitate publikoaren araubidea

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

eta Autonomia Erkidegoko Administrazioko Ogasun eta Herri Administrazio Sailaren ekonomia, finantza eta kudeaketa arloko kontrola; horrek denak ez du esan nahi ekonomia eta finantzetako eta kontularitzako jarduerak Herri Kontuen Euskal Epaitegiak kontrolatuko ez dizkionik.

14. artikulua.– Gobernu-organoak

Zuzendaria, Kontseilu Aholku-emailea eta bere estatutuan zehazturik dituenak dira Datuak Babesteko Euskal Bulegoaren gobernu-organoak.

15. artikulua.– Zuzendaria

1.– Zuzendariak zuzentzen eta ordezkatzen du Datuak Babesteko Euskal Bulegoa. Eusko Jaurlaritzaren dekretu baten bidez izendatuko dute, lau urterako.

2.– Inolako loturarik gabe eta objektibotasunez beteko ditu bere zereginak, eta ez du inolako jarraibiderik bete beharrik izango. Baina Kontseilu Aholkuemaileak, bere zereginak betetzean, ezer proposatzen badio, zuzendariak entzun egin beharko dio.

3.– Datuak Babesteko Euskal Bulegoko zuzendariak kargua epea amaitu baino lehenago uztekotan, honako arrazoi hauetakoren batengatik utziko du:

a) Berak eskaturik.

b) Gobernu Kontseiluak kargutik kentzea erabakita, arrazoi hauetakoren bat dela eta: betebehar larriak bete ez dituelako, bere lana egin ezina etorri zaiolako, bateraezintasunen bat dela-eta edo dolozko delituren batengatik epaia jaso duelako. Halakoetan, espedientea egin beharko da aurretiaz, eta Kontseilu Aholku-emaileari entzun beharko zaio, derrigor, espediente horretan.

4.– Datuak Babesteko Euskal Bulegoko zuzendaria goi-kargua izango da, aurretik eginkizun publikoren bat betetzen bazuen zerbitzu berezietan geratuko da, eta Autonomia Erkidegoko administrazioko goikarguen bateraezintasun-sistemaren pean egongo da.

16. artikulua.– Kontseilu Aholku-emailea

1.– Datuak Babesteko Euskal Bulegoak Kontseilu Aholku-emaile bat izango du, aholkuak emateko. Honako kide hauek izango ditu:

a) Eusko Legebiltzarreko ordezkari bat, Legebiltzarrak berak izendaturik.

b) Euskal Autonomia Erkidegoko Administrazioko ordezkari bat, Gobernu Kontseiluak izendaturik.

c) Lurralde historikoen ordezkari bat, lurralde horiek batera izendaturik.

d) Euskal Autonomia Erkidegoko lurraldeko tokierakundeetako ordezkari bat, lurralde horretan erakunde horien ordezkaritza handiena duen elkarteak izendaturik.

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) Bi aditu, bata informatikakoa eta bestea oinarrizko eskubideetakoa, Euskal Herriko Unibertsitateak izendaturik Euskal Autonomia Erkidegoko zuzenbide publikoko korporazioei galdetu ondoren.

2.– Kontseilu Aholku-emaileak berak onartuko ditu bere antolaketako eta funtzionamenduko arauak. Lehendakari-kargua eta idazkari-kargua egongo dira arau horietan aurreikusita, eta nola aukeratu edo izendatu behar diren ere bai.

17. artikulua.– Zereginak

1.– Lege honetako 2.1 artikuluan aipaturik datozen fitxategiak direla-eta, eta Euskal Autonomia Erkidegoaren aginpideen eremuan, hona hemen Datuak Babesteko Euskal Bulegoaren eginkizunak:

a) Datuak babesteko legeak bete daitezen zaintzea eta nola aplikatzen diren kontrolatzea, batez ere informaziorako eskubideari eta datuetara iristeko, datuak zuzentzeko, datuen aurka egiteko eta datuak indarrik gabe uzteko eskubideari dagokienez.

b) Lege eta erregelamenduetan zehazturik dauden baimenak ematea.

c) Beharrezkoa bada, datuen tratamendua datuak babesteko indarrean dagoen legediko printzipioetara egokitzeko beharrezko jarraibideak ematea, beste erakunde batzuen aginpideei ezer kendu gabe.

d) Tartean direnen eskariei eta erreklamazioei kasu egitea.

e) Datu pertsonalak tratatzea dela-eta dituzten eskubideei buruzko informazioa ematea pertsonei.

f) Tratamenduen erantzule eta arduradunei, esateko dutena entzun eta gero, datu-tratamendua indarrean dauden legeetara egokitzeko beharrezko neurriak hartzeko eskatzea, eta, beharrezkoa bada, ez badituzte lege horiek betetzen, tratamendua gelditzeko eta fitxategiak indarrik gabe uzteko agintzea, salbu datuen nazioarteko transferentziei buruzkoan.

g) Zehatzeko ahalmena erabiltzea, eta, beharrezkoa izanez gero, bere iritziz lege honetako 22. artikuluan tipifikaturiko arau-hausteen erantzuleak direnen aurka diziplinazko prozedura hasteko proposatzea, eta hartu beharreko zuhurtziako neurriak hartzea, salbu datuen nazioarteko transferentziei buruzkoan. Hori guztia lege honetan zehazturik dagoen moduan.

h) Lege hau garatzeko xedapen orokorretako egitasmoei buruzko txostenak egitea, derrigor.

i) Bere lana egiteko beharrezkoa duen laguntza eta informazio guztia eskatzea fitxategien erantzuleei.

j) Datu pertsonalen fitxategiak badirela gauza jakinekoa izan dadin zaintzea. Horretarako, urtero-urtero, fitxategi horien zerrenda bat argitaratuko du, beste

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

hainbat informazio osagarrirekin. Datuak Babesteko Euskal Bulegoko zuzendariak erabakiko du zein informazio osagarri eman.

k) Urteko txostena idatzi, eta Eusko Jaurlaritzako Lehendakariordetzara bidali.

l) Funtzio estatistiko publikoari buruzko legeek estatistikako datuen bilketari buruz eta estatistikako isilpekotasunari buruz dakartzaten xedapenak bete daitezen zaintzea, beharrezko jarraibideak ematea, estatistikarako bakarrik sortutako fitxategien segurtasun-baldintzei buruzko irizpenak ematea eta 24. artikuluan aipaturiko ahalmena erabiltzea.

m) Datu pertsonalen fitxategien segurtasuna eta herritarrek fitxategi horiei buruz dituzten eskubideak hobeto babeste aldera, Datuak Babesteko Estatuko Bulegoarekin eta beste autonomia-erkidego batzuetako antzeko erakundeekin lankidetzan aritzea hartarako beharrezkoak diren jarduera guztietan.

n) Lege honetako 2.1 artikuluko herri-administrazioek, erakundeek eta korporazioek datu pertsonalen babesari buruz egiten dizkioten galderei erantzutea, eta lege honen aplikazioaren pean dauden datu pertsonalen tratamenduari buruz beste pertsona fisiko edo juridiko batzuek egiten dizkioten galderei erantzutea.

ñ) Lege eta erregelamenduetan emandako beste eginkizun oro.

2.– Aurreko zenbakian zehaztu diren eginkizunak direla-eta, Datuak Babesteko Euskal Bulegoa kontroleko agintetzat hartuko da, eta lan horretan erabateko independentzia eta objektibotasuna izango du, legeak bermaturik.

18. artikulua.– Datuak Babesteko Erregistroa

1.– Datuak Babesteko Erregistroa sortzen da. Datuak Babesteko Euskal Bulegoaren barruan egongo da organo hori, bulegoaren estatutuetan zehazturiko moduan.

2.– Datuak Babesteko Erregistroan honako gauza hauek inskribatu beharko dira:

a) Lege honetako 2.1 artikuluan zehazturiko fitxategiak.

b) Datu pertsonalak babesteko abenduaren 13ko 15/1999 lege organikoan zehazturiko baimenak.

c) Inskribaturiko fitxategiei dagozkien ereduzko kodeak.

d) Inskribaturiko fitxategiei buruzko datu hauek: informazio-eskubidea, datuetara iristeko eskubidea, datuak zuzentzeko eskubidea, datuak indarrik gabe uzteko eskubidea eta aurka egiteko eskubidea erabiltzeko behar direnak.

3.– Baten batek inskribatzeko eskatu, baina Datuak Babesteko Erregistroak uste badu eskabide hori ez

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

dela zuzenbidearen araberakoa, ezezkoa erantzun dezake erregistroak. Halakoetan, Datuak Babesteko Euskal Bulegoko zuzendariak eskari-egileari beharrezko zuzenketak egiteko eskatu beharko dio.

4.– Lege honetako 2.1 artikuluan aipatutako fitxategiak Datuak Babesteko Erregistroan nola inskribatu behar diren, inskripzioen edukia, nola aldatu, indarrik gabe nola utzi, ebazpenen aurkako erreklamazioak eta errekurtsoak nola aurkeztu eta halako gainerako gorabeherak erregelamendu bidez arautuko dira.

5.– Edonork kontsulta dezake, dohainik, Datuak Babesteko Erregistroa. Behar duen informazioa erregistro horretan eskatuz, edonork jakin dezake datu pertsonalik tratatzen ari ote diren, zertarako ari diren hori egiten eta nor den arduraduna.

19. artikulua.– Ikuskapen-ahalmena

1.– Datuak Babesteko Euskal Bulegoak, kontroleko agintea denez, bere esku izango du lege honetako 2.1 artikuluan aipaturik dauden fitxategiak ikuskatzea. Bere lana egiteko behar duen informazio guztia bilduko du halakoetan. Horretarako, nahi badu, agiriak erakusteko edo bidaltzeko eska dezake, eta dauden tokian aztertu, eta datuak tratatzeko erabilitako tresna fisikoak eta logikoak ere azter ditzake, instalaturik dauden lokaletara joanda.

2.– Aurreko zenbakian aipatzen den ikuskatze-lana egiten duten funtzionarioak aginte publikotzat joko dira lan horretan ari direla; eta beren zereginak betetzen dihardutenean jakiten dutena isilpean gorde beharko dute derrigor, baita lan hori utzi eta gero ere.

20. artikulua.– Fitxategien titularrei errekerimendua egitea

Datuak Babesteko Euskal Bulegoko zuzendariak ikusten badu lege honen aplikaziopean dagoen halako fitxategi bat mantendu eta erabiltzeko modua lege honen beraren aginduren baten edo legea garatzen duen xedapenen baten aurkakoa dela, fitxategiaren titularra den herri-administrazio, erakunde edo korporaziora jo ahal izango du, errekerimendu bidez, eta zer zuzendu adierazi ahal izango dio, eta halako epetan zuzentzeko adierazi, gainera, berariaz. Errekerimendua jaso duen administrazioak ez baldin badu eskaturikoa betetzen, Datuak Babesteko Euskal Bulegoko zuzendariak administrazio horren ebazpen edo ezezko jarreraren aurkako errekurtsoa jarri ahal izango du, eta, halakoetan, interesduna izango da. Horrek ez du esan nahi lege honetako 17.f) artikuluaren arabera beste neurririk hartu ezin duenik.

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.

III. TITULUA

ZEHATZEKO ARAUBIDEA

21. artikulua.– Erantzuleak

Lege honetako 2.1 artikuluan aipaturik datozen fitxategien erantzuleak eta fitxategi horietako tratamenduen arduradunak lege honetan arau-hauste eta zehapenetarako zehazturik dauden arauen pean egongo dira.

22. *artikulua.*– Arau-hauste motak

1.– Arau-hausteak arinak, larriak edo oso larriak izango dira.

2.– Hauek dira arau-hauste arinak:

a) Interesdunak eskatzen badu tratatzen ari diren datu pertsonalak zuzentzeko edo indarrik gabe uzteko, eta legez hala egin behar bada, eskari horri kasurik ez egitea forma-arrazoiengatik.

b) Datuen babesarekin zerikusi funtsezkoa ez duten gauzetan, Datuak Babesteko Euskal Bulegoak halako informazio bat eskatzen duenean legez dagozkion aginpideak bete beharrez, informazio hori ez ematea.

c) Datu pertsonalen fitxategia Datuak Babesteko Erregistroan inskribatzeko eskaria ez egitea, non eta ez den arau-hauste larria.

d) Tartean direnengandik, legez eman beharreko informazioa eman gabe jasotzea zuzenean datu pertsonalak.

e) Isilpekotasuna, legezko betebeharra baita, apurtzea, non eta ez den arau-hauste larria.

3.– Hauek dira arau-hauste larriak:

a) Fitxategiak sortzen edo fitxategi horietarako datu pertsonalak biltzen hastea, xedapen orokor bidezko baimenik gabe. Xedapen horrek Euskal Herriko Agintaritzaren Aldizkarian edo dena delako lurralde historikoan argitaraturik agertu beharko du.

b) Datu pertsonalak biltzen hastea, tartean direnen oniritzi berariazkoa eskatu gabe, oniritzi hori beharrezkoa denetan.

c) Legezko printzipio eta bermeak urraturik edo garapeneko erregelamenduetan datozen babes-aginduak bete gabe tratatzea, edo erabiltzea gero, datu pertsonalak, non eta ez den oso arau-hauste larria.

d) Datuetara iristeko eta datuen aurka egiteko eskubideari bidea ixtea edo oztopoak jartzea eta eskatutako informazioa emateari uko egitea.

e) Datu pertsonalak babesteko legeen babespean diren pertsonen eskubideei erasaten bazaie, erabat zuzenak ez diren datu pertsonalak mantentzea edo datu horiek direla-eta legez egin beharreko zuzenketak edo indargabetzeak ez egitea.

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) Fitxategietan jasotako datu pertsonalak isilpean gorde beharra ez betetzea administrazio- edo zigor-arloko arau-hausteei buruzko datuak badira, edo herri-ogasunari buruzkoak badira, bai eta inoren izaerari antzemateko behar beste datu pertsonal duen beste edozein fitxategitako datuak badira ere.

g) Datu pertsonalak dauzkaten fitxategiak, lokalak, programak edo ekipoak beharrezko segurtasun-neurririk gabe edukitzea.

h) Lege eta erregelamenduetan zehazturiko komunikazioak Datuak Babesteko Euskal Bulegora ez bidaltzea, eta jaso behar dituen edo eskatzen dituen agiri eta informazioak ez ematea.

i) Ikuskatze-lanei oztopoak jartzea.

j) Datu pertsonalen fitxategia ez inskribatzea Datuak Babesteko Erregistroan, Datuak Babesteko Euskal Bulegoko zuzendariak hala eskatu badu.

k) Datuak beste batengandik jaso badira, tartean dagoena ez den beste batengandik, legez eman beharreko informazioa ez ematea.

4.– Hauek dira oso arau-hauste larriak:

a) Datuak engainu edo iruzur bidez biltzea.

b) Datu pertsonalak inori jakinaraztea edo uztea, hartarako baimenik ez dagoenean.

c) Tartean denak hartarako oniritzirik eman ez badu berariaz, ideologiaren, sindikatu-bazkidetzaren, erlijioaren edo sineskeren berri ematen duten datu pertsonalak biltzea eta tratatzea.

d) Legez hala egin behar ez bada edo tartean denak hartarako oniritzirik eman ez badu berariaz, arrazari, osasunari edo bizimodu sexualari buruzko datuak biltzea eta tratatzea.

e) Ideologia, sindikatu-bazkidetza, erlijioa, sineskerak, arraza, etnia edo bizimodu sexuala adierazten duten datu pertsonalak jasotzeko bakarrik sortzea fitxategiak.

f) Datuak Babesteko Euskal Bulegoko zuzendariak edo datuetara iristeko eskubidearen titularrak eskatu arren ez jarraitzeko horrela, datu pertsonalei legez kanpoko tratamendua ematen jarraitzea.

g) Oinarrizko eskubideak erabiltzea galarazten edo oztopatzen bada horrela, datu pertsonalak lege onez ez tratatzea edo aplikatu behar zaizkien printzipio eta bermeei muzin eginda tratatzea.

h) Paragrafo honetako bertako e) letran zehazturiko datu pertsonalak edo tartean denak oniritzia eman gabe polizia-lanerako bildu direnak isilpean gorde beharra urratzea.

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) Datuetara iristeko, datuak zuzentzeko, indarrik gabe uzteko eta datuen aurka egiteko eskubideak behin eta berriz aintzakotzat ez hartzea edo oztopatzea.

j) Inoren datu pertsonalak fitxategi batean sartzerakoan, legearen arabera egin beharreko jakinarazpena sistemaz ez egitea.

5.– Artikulu honetan egin den arau-hausteen tipifikazioa gorabehera, Euskal Autonomia Erkidegoak aginpiderik ez duen gaietan datuen babesari buruzko Estatuko legeetako tipifikazioek bere hartan irauten dute.

23. artikulua.– Zigor-motak

1.– 601,01 eta 60.101,21 euro bitarteko isuna arau-hauste arinengatik.

2.– 60.101,21 eta 300.506,05 euro bitarteko isuna arau-hauste larriengatik.

3.– 300.506,05 eta 601.012,1 euro bitarteko isuna oso arau-hauste larriengatik.

4.– Zigorren zenbatekoa zehazteko, honako gauza hauek hartuko dira kontuan: erasandako eskubide pertsonalak nolakoak diren, tratamenduen zenbatekoa, lortutako irabaziak, arau-hausteak zenbateraino diren nahita egindakoak, behin baino gehiagotan egin ote diren, interesdunei eta beste batzuei (hirugarrenei) eragindako kalte-galerak eta dena delako arau-haustea zenbateraino den legez kanpokoa zehazteko eta zenbateraino erruduntasuna dagoen zehazteko garrantzitsua den beste edozein gorabehera.

5.– Tartean diren gorabeherak gogoan harturik, ikusten bada inputatuaren errua uste baino dezente txikiagoa dela edo arau-hausteak dezente gutxiago urratzen dituela legeak, berez legokiokeen arau-hauste motako eskala baino justu arau-hauste arinagoen motako eskala aplikatuz zehaztuko du zigorraren zenbatekoa erakunde zigortzaileak.

6.– Ezin da, inola ere ez, zigortu nahi den arau-hauste motari legez dagokion zigorra baino larriagorik jarri.

7.– Eusko Jaurlaritzak, aldika-aldika, zigorren zenbatekoa eguneratu egingo du, prezioen indizeen aldaketen arabera.

24. artikulua.– Herri-administrazioek, erakundeek eta Zuzenbide publikoko korporazioek egindako arau-hausteak

1.– Dagokion prozedura-instrukzioa egin, eta aurreko artikuluko arau-hausteetakoren bat edo batzuk gertatu direla ikusiz gero ondorio modura –lege honetako 2.1 artikuluko fitxategiei dagokienez–, Datuak Babesteko Euskal Bulegoko zuzendariak, ebazpen bidez, arau-haustearen ondorioak gerarazteko edo zuzentzeko beharrezko neurriak aginduko ditu. Ebazpen hori fitxategiaren erantzuleari, hierarkiaz gainetik duen erakundeari eta –halakorik baldin badago– tartean di-

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 fi-

renei jakinarazi behar zaie, eta ebazpen horrek amaitzen du administrazio-bidea.

2.– Datuak Babesteko Euskal Bulegoko zuzendariak, diziplinazko bidetik jotzeko ere proposa dezake, hala badagokio. Herri-administrazioetan eta lege honetako 2.1 artikuluan aipatutako erakunde eta korporazioetan lan egiten duten funtzionarioen eta langileen diziplina-araubidea zehazten duten legeetan ezarritakoak izango dira erabili beharreko prozedura eta jarri beharreko zigorrak. Ondorio horietarako, lege honetan tipifikaturiko arau-hausteak aplikatu beharreko diziplina-araubidearen osagarri izango dira.

3.– Zigor-prozedurarik behar izanez gero, Euskal Autonomia Erkidegoko Herri Administrazioen Zigortzeko Ahalmenari buruzko otsailaren 20ko 2/1998 Legean jartzen duena bete beharko da.

4.– Aurreko puntuetan aipatzen diren neurri eta jarduerak direla-eta ematen diren ebazpenak Datuak Babesteko Euskal Bulegoari jakianarazi beharko zaizkio.

5.– Datuak Babesteko Euskal Bulegoko zuzendariak Arartekoari jakinarazi beharko dizkio aurreko puntu horietaz baliatuz egiten dituen jarduerak eta ematen dituen ebazpenak.

25. atala.– Fitxategiak geldiaraztea

Inork beste inoren datu pertsonalak legez kanpo erabiltzen edo uzten baditu, oso arau-hauste larria egiteko moduan, eta, horrenbestez, jokaera horrek traba eta eragozpen larriak badakartza herritarren eskubideen erabilerarako eta nortasuna askatasunez garatzeko –bai Konstituzioan bai legeetan bermaturik daude erabilera eta garapen horiek–, Datuak Babesteko Euskal Bulegoko zuzendariak datu pertsonalen fitxategien erantzuleei eska diezaieke aurrerantzean daturik ez erabiltzeko edo uzteko legez kanpo. Ez baldin badiote errekerimenduari kasu egiten, fitxategi horiek geldirazi egin ditzake ebazpen arrazoitu bidez, tartean direnen eskubideak atzera ezartzeko, eta horretarako bakarrik.

XEDAPEN GEHIGARRIAK

Lehena.– Fitxategien berri Datuak Babesteko Euskal Bulegoari ematea

Lege honetako 2.1) artikuluan aipaturik dauden herri-administrazioek, erakundeek eta korporazioek, agindu horretan aipaturiko fitxategien titular badira, Datuak Babesteko Euskal Bulegoari eman beharko diote haren berri, lege hau indarrean jarri eta hiru hilabeteko epean. Hori baino lehenago, kasuan kasuko fitxategia arautzeko xedapena onarturik eta argitaraturik izan behar dute.

chero, 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.

Bigarrena.– Erroldako datuak jakinaraztea

1.– Datu Pertsonalak Babesteko abenduaren 13ko 15/1999 Lege Organikoko bigarren xedapen gehigarrian eta Toki Jaurbidearen Oinarriak Arautzen dituen apirilaren 2ko 7/1985 Legeko 17.3 artikuluan zehazturik dagoen moduan,Euskal Autonomia Erkidegoko Administrazio orokorrak eta foru-administrazioek, biztanleen fitxategiak edo erregistroak sortze aldera, Euskal Estatistika Erakundeari aginpideak dauzkaten lurraldeetako biztanleen udal-erroldetan dauden fitxategien kopia eguneratu bat eska diezaiokete, interesdunaren oniritziaren beharrik gabe, honako datu hauek eskuratzeko: izena, abizenak, helbidea, sexua eta jaiotze-eguna. Komunikaziorako balioko dute biztanleen fitxategi edo erregistro horiek, hau da, herri-administrazio bakoitzeko organoen eta dagokien lurraldean bizi diren interesdunen arteko komunikaziorako, herri-administrazio bakoitzaren aginpideetatik datozen harreman juridiko-administratiboei dagokionez.

2.– Aurreko paragrafoan xedaturikoaren ondorioetarako, Euskal Autonomia Erkidegoko Estatistikari buruzko apirilaren 28ko 4/1986 Legeko 29. artikulua aldatu, eta honela gelditzen da: agindu horren gaur egungo idazkera aginduaren 1. zenbakia izango da aurrerantzean, eta honako 2. zenbaki hau gehitzen zaio:

«2. Euskal Estatistika Erakundeak Euskal Autonomia Erkidegoko udalerri guztietako udal-errolden kopien gordetzaile-lana ere egingo du, eta, horretarako, udalerriek administrazio-erregistro horien kopiak bidali beharko dizkiote erregelamendu bidez zehaztutako moduan».

Hirugarrena.– Ararteko aren eta Datuak Babesteko Estatuko Bulegoaren aginpideak

Lege honetan xedaturikoa gorabehera Ararteko aren eta Datuak Babesteko Estatuko Bulegoaren aginpideek bere hartan diraute.

AZKEN XEDAPENA

Nola garatu eta aplikatu

1.– Lege honetan xedaturikoa garatzeko eta aplikatzeko baimena du Eusko Jaurlaritzak.

2.– Beharrezko aurrekontu-atala sortzeko eta, Euskal Autonomia Erkidegoko aurrekontu-araubidea antolatzen duten legeekin bat, aurrekontua lege honetan xedaturikoa aplikatzeko behar beste aldatzeko baimena du Ogasun eta Herri Administrazio Sailak.

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 términos: 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.

Beraz, Lege honi men egiteko eta men eginarazteko agintzen diet, norbanako zein agintari direla, Euskadiko herritar guztiei.

Vitoria-Gasteiz, 2004ko otsailaren 26a.

Lehendakaria,
JUAN JOSÉ IBARRETXE MARKUARTU.

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

Dado en Vitoria-Gasteiz, a 26 de febrero de 2004.

El Lehendakari,
JUAN JOSÉ IBARRETXE MARKUARTU.

GIPUZKOAKO FORU ALDUNDIA

Zk-1185

18/2003 FORU ARAUA, abenduaren 15ekoa, Prestige itsasontziaren istripua dela eta emandako laguntza publikoak hainbat zergatatik salbuesten dituena.

GIPUZKOAKO DIPUTATU NAGUSIAK

Jakinarazten dut Gipuzkoako Batzar Nagusiek onartu dutela «Prestige itsasontziaren istripua dela eta emandako laguntza publikoak hainbat zergatatik salbuesten dituen abenduaren 15eko 18/2003 Foru Araua», eta nik aldarrikatu eta argitara dadin agintzen dut aplikagarria zaien herritar guztiek, partikularrek nahiz agintariek, bete eta betearazi dezaten.

Donostia, 2003ko abenduaren 15a.

Diputatu Nagusia,
JOXE JOAN GONZALEZ DE TXABARRI MIRANDA.

HITZAURREA

Prestige itsasontziak 2002ko azaroaren 13an izandako istripuaren ondorioz, kaltetutako zonetako herri administrazioek jarduketa jakin batzuk egin behar izan dituzte hondamendiak ingurumenean eta arlo ekonomiko eta sozialean eragin dituen ondorioei aurre egiteko.

Gertaeren tamaina eta istripuaren eragin kaltegarriak ikusita, mota askotako neurriak hartu behar izan dira arazoak arindu eta ahal den neurrian konpontzearren. Laguntza ekonomikoak ematea izan da neurri horietako bat, bai istripuaren ondorioz kaltetutakoei banatu zaizkienak eta bai kalte horiek konpontzeko neurriak hartzeko eman direnak.

Bada, foru arau honen xedea da aitortzea istripu horren ondorioz kaltetuta gertatu direnek jasotako lagun-

DIPUTACIÓN FORAL DE GIPUZKOA

Nº-1185

NORMA FORAL 18/2003 de 15 de diciembre por la que se declara la exención fiscal de las ayudas publicas concedidas como consecuencia del accidente del buque Prestige.

EL DIPUTADO GENERAL DE GIPUZKOA

Hago saber que las Juntas Generales de Gipuzkoa han aprobado y yo promulgo y ordeno la publicación de la siguiente «Norma Foral 18/2003 de 15 de diciembre por la que se declara la exención fiscal de las ayudas públicas concedidas como consecuencia del accidente del buque Prestige» a los efectos de que todos los ciudadanos, particulares y autoridades a quienes sea de aplicación la guarden y hagan guardarla.

Donostia-San Sebastián, 15 de diciembre de 2003.

El Diputado General,
JOXE JOAN GONZALEZ DE TXABARRI MIRANDA.

PREÁMBULO

Como consecuencia del accidente sufrido por el buque «Prestige» el 13 de noviembre de 2002, las Administraciones públicas de las zonas afectadas se han visto obligadas a efectuar determinadas actuaciones al objeto de paliar el impacto medioambiental, económico y social originado por dicha catástrofe.

La magnitud de los hechos y los efectos perjudiciales del accidente han exigido la adopción de medidas paliativas y reparadoras de diversa índole, tales como la concesión de ayudas económicas para los perjudicados por el accidente o para la adopción de medidas reparadoras de los citados perjuicios.

El objeto de la presente Norma Foral es declarar la exención en el Impuesto sobre la Renta de las Personas

Osakidetza

Ley 41/2002,

de 14 de diciembre, Básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica

Septiembre 2007

LEY 41/2002, DE 14 DE NOVIEMBRE, BÁSICA REGULADORA DE LA AUTONOMÍA DEL PACIENTE Y DE DERECHOS Y OBLIGACIONES EN MATERIA DE INFORMACIÓN Y DOCUMENTACIÓN CLÍNICA.

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley.

EXPOSICIÓN DE MOTIVOS

La importancia que tienen los derechos de los pacientes como eje básico de las relaciones clínico-asistenciales se pone de manifiesto al constatar el interés que han demostrado por los mismos casi todas las organizaciones internacionales con competencia en la materia. Ya desde el fin de la Segunda Guerra Mundial, organizaciones como Naciones Unidas, UNESCO o la Organización Mundial de la Salud, o, más recientemente, la Unión Europea o el Consejo de Europa, entre muchas otras, han impulsado declaraciones o, en algún caso, han promulgado normas jurídicas sobre aspectos genéricos o específicos relacionados con esta cuestión. En este sentido, es necesario mencionar la trascendencia de la Declaración universal de derechos humanos, del año 1948, que ha sido el punto de referencia obligado para todos los textos constitucionales promulgados posteriormente o, en el ámbito más estrictamente sanitario, la Declaración sobre la promoción de los derechos de los pacientes en Europa, promovida el año 1994 por la Oficina Regional para Europa de la Organización Mundial de la Salud, aparte de múltiples declaraciones internacionales de mayor o menor alcance e influencia que se han referido a dichas cuestiones.

Últimamente, cabe subrayar la relevancia especial del Convenio del Consejo de Europa para la protección de los derechos humanos y la dignidad del ser humano respecto de las aplicaciones de la biología y la medicina (Convenio sobre los derechos del hombre y la biomedicina), suscrito el día 4 de abril de 1997, el cual ha entrado en vigor en el Reino de España el 1 de enero de 2000. Dicho Convenio es una iniciativa capital: en efecto, a diferencia de las distintas declaraciones internacionales que lo han precedido, es el primer instrumento internacional con carácter jurídico vinculante para los países que lo suscriben. Su especial valía reside en el hecho de que establece un marco común para la protección de los derechos humanos y la dignidad humana en la aplicación de la biología y la medicina. El Convenio trata explícitamente, con detenimiento y extensión, sobre la necesidad de reconocer los derechos de los pacientes, entre los cuales resaltan el derecho a la información, el consentimiento informado y la intimidad de la información relativa ala salud de las personas, persiguiendo el alcance de una armonización de las legislaciones de los diversos países en estas materias; en este sentido, es absolutamente conveniente tener en cuenta el Convenio en el momento de abordar el reto de regular cuestiones tan importantes.

Es preciso decir, sin embargo, que la regulación del derecho a la protección de la salud, recogido por el artículo 43 de la Constitución de 1978, desde el punto de vista de las

cuestiones más estrechamente vinculadas a la condición de sujetos de derechos de las personas usuarias de los servicios sanitarios, es decir, la plasmación de los derechos relativos a la información clínica y la autonomía individual de los pacientes en lo relativo a su salud, ha sido objeto de una regulación básica en el ámbito del Estado, a través de la Ley 14/1986, de 25 de abril, General de Sanidad.

De otra parte, esta Ley, a pesar de que fija básicamente su atención en el establecimiento y ordenación del sistema sanitario desde un punto de vista organizativo, dedica a esta cuestión diversas previsiones, entre las que destaca la voluntad de humanización de los servicios sanitarios. Así mantiene el máximo respeto ala dignidad de la persona y a la libertad individual, de un lado, y, del otro, declara que la organización sanitaria debe permitir garantizar la salud como derecho inalienable de la población mediante la estructura del Sistema Nacional de Salud, que debe asegurarse en condiciones de escrupuloso respeto a la intimidad personal y ala libertad individual del usuario, garantizando la confidencialidad de la información relacionada con los servicios sanitarios que se prestan y sin ningún tipo de discriminación.

A partir de dichas premisas, la presente Ley completa las previsiones que la Ley General de Sanidad enunció como principios generales. En este sentido, refuerza y da un trato especial al derecho a la autonomía del paciente. En particular, merece mención especial la regulación sobre instrucciones previas que contempla, de acuerdo con el criterio establecido en el Convenio de Oviedo, los deseos del paciente expresados con anterioridad dentro del ámbito del consentimiento informado. Asimismo, la Ley trata con profundidad todo lo referente a la documentación clínica generada en los centros asistenciales, subrayando especialmente la consideración y la concreción de los derechos de los usuarios en este aspecto.

En septiembre de 1997, en desarrollo de un convenio de colaboración entre el Consejo General del Poder Judicial y el Ministerio de Sanidad y Consumo, tuvo lugar un seminario conjunto sobre información y documentación clínica, en el que se debatieron los principales aspectos normativos y judiciales en la materia. Al mismo tiempo, se constituyó un grupo de expertos a quienes se encargó la elaboración de unas directrices para el desarrollo futuro de este tema. Este grupo suscribió un dictamen el 26 de noviembre de 1997, que ha sido tenido en cuenta en la elaboración de los principios fundamentales de esta Ley.

La atención que a estas materias otorgó en su día la Ley General de Sanidad supuso un notable avance como reflejan, entre otros, sus artículos 9, 10 y 61. Sin embargo, el derecho a la información, como derecho del ciudadano cuando demanda la atención sanitaria, ha sido objeto en los últimos años de diversas matizaciones y ampliaciones por Leyes y disposiciones de distinto tipo y rango, que ponen de manifiesto la necesidad de una reforma y actualización de la normativa contenida en la Ley General de Sanidad. Así, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, califica a los datos relativos a la salud de los ciudadanos como datos especialmente protegidos, estableciendo un régimen singularmente riguroso para su obtención, custodia y eventual cesión. Esta defensa de la confidencialidad había sido ya defendida por la Directiva comunitaria 95/46, de 24 de octubre, en la que, además de reafirmarse la defensa de los derechos y libertades de los ciudadanos europeos, en especial de su intimidad relativa a la información relacionada con su salud, se apunta la presencia de otros intereses generales como los estudios epidemiológicos, las

situaciones de riesgo grave para la salud de la colectividad, la investigación y los ensayos clínicos que, cuando estén incluidos en normas de rango de Ley, pueden justificar una excepción motivada a los derechos del paciente. Se manifiesta así una concepción comunitaria del derecho a la salud, en la que, junto al interés singular de cada individuo, como destinatario por excelencia de la información relativa ala salud, aparecen también otros agentes y bienes jurídicos referidos a la salud pública, que deben ser considerados, con la relevancia necesaria, en una sociedad democrática avanzada. En esta línea, el Consejo de Europa, en su Recomendación de 13 de febrero de 1997, relativa a la protección de los datos médicos, después de afirmar que deben recogerse y procesarse con el consentimiento del afectado, indica que la información puede restringirse si así lo dispone una Ley y constituye una medida necesaria por razones de interés general.

Todas estas circunstancias aconsejan una adaptación de la Ley General de Sanidad con el objetivo de aclarar la situación jurídica y los derechos y obligaciones de los profesionales sanitarios, de los ciudadanos y de las instituciones sanitarias. Se trata de ofrecer en el terreno de la información y la documentación clínicas las mismas garantías a todos los ciudadanos del Estado, fortaleciendo con ello el derecho a la protección de la salud que reconoce la Constitución.

CAPÍTULO I

Principios generales

Artículo 1. Ámbito de aplicación

La presente Ley tiene por objeto la regulación de los derechos y obligaciones de los pacientes, usuarios y profesionales, así como de los centros y servicios sanitarios, públicos y privados, en materia de autonomía del paciente y de información y documentación clínica.

Artículo 2. Principios básicos

1. La dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica.

2. Toda actuación en el ámbito de la sanidad requiere, con carácter general, el previo consentimiento de los pacientes o usuarios. El consentimiento, que debe obtenerse después de que el paciente reciba una información adecuada, se hará por escrito en los supuestos previstos en la Ley.

3. El paciente o usuario tiene derecho a decidir libremente, después de recibir la información adecuada, entre las opciones clínicas disponibles.

4. Todo paciente o usuario tiene derecho a negarse al tratamiento, excepto en los casos determinados en la Ley. Su negativa al tratamiento constará por escrito.

5. Los pacientes o usuarios tienen el deber de facilitar los datos sobre su estado físico o sobre su salud de manera leal y verdadera, así como el de colaborar en su obtención,

especialmente cuando sean necesarios por razones de interés público o con motivo de la asistencia sanitaria.

6. Todo profesional que interviene en la actividad asistencial está obligado no sólo a la correcta prestación de sus técnicas, sino al cumplimiento de los deberes de información y de documentación clínica, y al respeto de las decisiones adoptadas libre y voluntariamente por el paciente.

7. La persona que elabore o tenga acceso ala información y la documentación clínica está obligada a guardar la reserva debida.

Artículo 3. Las definiciones legales

A efectos de esta Ley se entiende por:

Centro sanitario: el conjunto organizado de profesionales, instalaciones y medios técnicos que realiza actividades y presta servicios para cuidar la salud de los pacientes y usuarios.

Certificado médico: la declaración escrita de un médico que da fe del estado de salud de una persona en un determinado momento.

Consentimiento informado: la conformidad libre, voluntaria y consciente de un paciente, manifestada en el pleno uso de sus facultades después de recibir la información adecuada, para que tenga lugar una actuación que afecta a su salud.

Documentación clínica: el soporte de cualquier tipo o clase que contiene un conjunto de datos e informaciones de carácter asistencial.

Historia clínica: el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial.

Información clínica: todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla.

Informe de alta médica: el documento emitido por el médico responsable en un centro sanitario al finalizar cada proceso asistencial de un paciente, que especifica los datos de éste, un resumen de su historial clínico, la actividad asistencial prestada, el diagnóstico y las recomendaciones terapéuticas.

Intervención en el ámbito de la sanidad: toda actuación realizada con fines preventivos, diagnósticos, terapéuticos, rehabilitadores o de investigación.

Libre elección: la facultad del paciente o usuario de optar, libre y voluntariamente, entre dos o más alternativas asistenciales, entre varios facultativos o entre centros asistenciales, en los términos y condiciones que establezcan los servicios de salud competentes, en cada caso.

Médico responsable: el profesional que tiene a su cargo coordinar la información y la asistencia sanitaria del paciente o del usuario, con el carácter de interlocutor principal del mismo en todo lo referente a su atención e información durante el proceso asistencial, sin perjuicio de las obligaciones de otros profesionales que participan en las actuaciones asistenciales.

Paciente: la persona que requiere asistencia sanitaria y está sometida a cuidados profesionales para el mantenimiento o recuperación de su salud.

Servicio sanitario: la unidad asistencial con organización propia, dotada de los recursos técnicos y del personal cualificado para llevar a cabo actividades sanitarias.

Usuario: la persona que utiliza los servicios sanitarios de educación y promoción de la salud, de prevención de enfermedades y de información sanitaria.

CAPÍTULO II

El derecho de información sanitaria

Artículo 4. Derecho a la información asistencial

1. Los pacientes tienen derecho a conocer, con motivo de cualquier actuación en el ámbito de su salud, toda la información disponible sobre la misma, salvando los supuestos exceptuados por la Ley. Además, toda persona tiene derecho a que se respete su voluntad de no ser informada. La información, que como regla general se proporcionará verbalmente dejando constancia en la historia clínica, comprende, como mínimo, la finalidad y la naturaleza de cada intervención, sus riesgos y sus consecuencias.

2. La información clínica forma parte de todas las actuaciones asistenciales, será verdadera, se comunicará al paciente de forma comprensible y adecuada a sus necesidades y le ayudará a tomar decisiones de acuerdo con su propia y libre voluntad.

3. El médico responsable del paciente le garantiza el cumplimiento de su derecho a la información. Los profesionales que le atiendan durante el proceso asistencial o le apliquen una técnica o un procedimiento concreto también serán responsables de informarle.

Artículo 5. Titular del derecho a la información asistencial

1. El titular del derecho ala información ese¡ paciente. También serán informadas las personas vinculadas a él, por razones familiares o de hecho, en la medida que el paciente lo permita de manera expresa o tácita.

2. El paciente será informado, incluso en caso de incapacidad, de modo adecuado a sus posibilidades de comprensión, cumpliendo con el deber de informar también a su representante legal.

3. Cuando el paciente, según el criterio del médico que le asiste, carezca de capacidad para entender la información a causa de su estado físico o psíquico, la información se

pondrá en conocimiento de las personas vinculadas a él por razones familiares o de hecho.

4. El derecho a la información sanitaria de los pacientes puede limitarse por la existencia acreditada de un estado de necesidad terapéutica. Se entenderá por necesidad terapéutica la facultad del médico para actuar profesionalmente sin informar antes al paciente, cuando por razones objetivas el conocimiento de su propia situación pueda perjudicar su salud de manera grave. Llegado este caso, el médico dejará constancia razonada de las circunstancias en la historia clínica y comunicará su decisión a las personas vinculadas al paciente por razones familiares o de hecho.

Artículo 6. Derecho a la información epidemiológica

Los ciudadanos tienen derecho a conocer los problemas sanitarios de la colectividad cuando impliquen un riesgo para la salud pública o para su salud individual, y el derecho a que esta información se difunda en términos verdaderos, comprensibles y adecuados para la protección de la salud, de acuerdo con lo establecido por la Ley.

CAPÍTULO III

Derecho a la intimidad

Artículo 7. El derecho a la intimidad

1. Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.

2. Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes.

CAPÍTULO IV

El respeto de la autonomía del paciente

Artículo 8. Consentimiento informado

1. Toda actuación en el ámbito de la salud de un paciente necesita el consentimiento libre y voluntario del afectado, una vez que, recibida la información prevista en el artículo 4, haya valorado las opciones propias del caso.

2. El consentimiento será verbal por regla general. Sin embargo, se prestará por escrito en los casos siguientes: intervención quirúrgica, procedimientos diagnósticos y terapéuticos invasores y, en general, aplicación de procedimientos que suponen riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente.

3. El consentimiento escrito del paciente será necesario para cada una de las actuaciones especificadas en el punto anterior de este artículo, dejando a salvo la posibilidad de incorporar anejos y otros datos de carácter general, y tendrá información suficiente sobre el procedimiento de aplicación y sobre sus riesgos.

4. Todo paciente o usuario tiene derecho a ser advertido sobre la posibilidad de utilizar los procedimientos de pronóstico, diagnóstico y terapéuticos que se le apliquen en un proyecto docente o de investigación, que en ningún caso podrá comportar riesgo adicional para su salud.

5. El paciente puede revocar libremente por escrito su consentimiento en cualquier momento.

Artículo 9. Límites del consentimiento informado y consentimiento por representación

1. La renuncia del paciente a recibir información está limitada por el interés de la salud del propio paciente, de terceros, de la colectividad y por las exigencias terapéuticas del caso. Cuando el paciente manifieste expresamente su deseo de no ser informado, se respetará su voluntad haciendo constar su renuncia documentalmente, sin perjuicio de la obtención de su consentimiento previo para la intervención.

2. Los facultativos podrán llevar a cabo las intervenciones clínicas indispensables en favor de la salud del paciente, sin necesidad de contar con su consentimiento, en los siguientes casos:

a) Cuando existe riesgo para la salud pública a causa de razones sanitarias establecidas por la Ley. En todo caso, una vez adoptadas las medidas pertinentes, de conformidad con lo establecido en la Ley Orgánica 3/1986, se comunicarán ala autoridad judicial en el plazo máximo de 24 horas siempre que dispongan el internamiento obligatorio de personas.

b) Cuando existe riesgo inmediato grave para la integridad física o psíquica del enfermo y no es posible conseguir su autorización, consultando, cuando las circunstancias lo permitan, a sus familiares o a las personas vinculadas de hecho a él.

3. Se otorgará el consentimiento por representación en los siguientes supuestos:

a) Cuando el paciente no sea capaz de tomar decisiones, a criterio del médico responsable de la asistencia, o su estado físico o psíquico no le permita hacerse cargo de su situación. Si el paciente carece de representante legal, el consentimiento lo prestarán las personas vinculadas a él por razones familiares o de hecho.

b) Cuando el paciente esté incapacitado legalmente.

c) Cuando el paciente menor de edad no sea capaz intelectual ni emocionalmente de comprender el alcance de la intervención. En este caso, el consentimiento lo dará el representante legal del menor después de haber escuchado su opinión si tiene doce años cumplidos. Cuando se trate de menores no incapaces ni incapacitados, pero emancipados o con dieciséis años cumplidos, no cabe prestar el consentimiento por

representación. Sin embargo, en caso de actuación de grave riesgo, según el criterio del facultativo, los padres serán informados y su opinión será tenida en cuenta para la toma de la decisión correspondiente.

4. La interrupción voluntaria del embarazo, la práctica de ensayos clínicos y la práctica de técnicas de reproducción humana asistida se rigen por lo establecido con carácter general sobre la mayoría de edad y por las disposiciones especiales de aplicación.

5. La prestación del consentimiento por representación será adecuada a las circunstancias y proporcionada a las necesidades que haya que atender, siempre en favor del paciente y con respeto a su dignidad personal. El paciente participará en la medida de lo posible en la toma de decisiones a lo largo del proceso sanitario.

Artículo 10. Condiciones de la información y consentimiento por escrito

1. El facultativo proporcionará al paciente, antes de recabar su consentimiento escrito, la información básica siguiente:

a) Las consecuencias relevantes o de importancia que la intervención origina con seguridad.

b) Los riesgos relacionados con las circunstancias personales o profesionales del paciente.

c) Los riesgos probables en condiciones normales, conforme ala experiencia y al estado de la ciencia o directamente relacionados con el tipo de intervención.

d) Las contraindicaciones.

2. El médico responsable deberá ponderar en cada caso que cuanto más dudoso sea el resultado de una intervención más necesario resulta el previo consentimiento por escrito del paciente.

Artículo 11. Instrucciones previas

1. Por el documento de instrucciones previas, una persona mayor de edad, capaz y libre, manifiesta anticipadamente su voluntad, con objeto de que ésta se cumpla en el momento en que llegue a situaciones en cuyas circunstancias no sea capaz de expresarlos personalmente, sobre los cuidados y el tratamiento de su salud o, una vez llegado el fallecimiento, sobre el destino de su cuerpo o de los órganos del mismo. El otorgante del documento puede designar, además, un representante para que, llegado el caso, sirva como interlocutor suyo con el médico o el equipo sanitario para procurar el cumplimiento de las instrucciones previas.

2. Cada servicio de salud regulará el procedimiento adecuado para que, llegado el caso, se garantice el cumplimiento de las instrucciones previas de cada persona, que deberán constar siempre por escrito.

3. No serán aplicadas las instrucciones previas contrarias al ordenamiento jurídico, a la «lex artis», ni las que no se correspondan con el supuesto de hecho que el interesado

haya previsto en el momento de manifestarlas. En la historia clínica del paciente quedará constancia razonada de las anotaciones relacionadas con estas previsiones.

4. Las instrucciones previas podrán revocarse libremente en cualquier momento dejando constancia por escrito.

5. Con el fin de asegurar la eficacia en todo el territorio nacional de las instrucciones previas manifestadas por los pacientes y formalizadas de acuerdo con lo dispuesto en la legislación de las respectivas Comunidades Autónomas, se creará en el Ministerio de Sanidad y Consumo el Registro nacional de instrucciones previas que se regirá por las normas que reglamentariamente se determinen, previo acuerdo del Consejo Interterritorial del Sistema Nacional de Salud.

Artículo 12. Información en el Sistema Nacional de Salud

1. Además de los derechos reconocidos en los artículos anteriores, los pacientes y los usuarios del Sistema Nacional de Salud tendrán derecho a recibir información sobre los servicios y unidades asistenciales disponibles, su calidad y los requisitos de acceso a ellos.

2. Los servicios de salud dispondrán en los centros y servicios sanitarios de una guía o carta de los servicios en la que se especifiquen los derechos y obligaciones de los usuarios, las prestaciones disponibles, las características asistenciales del centro o del servicio, y sus dotaciones de personal, instalaciones y medios técnicos. Se facilitará a todos los usuarios información sobre las guías de participación y sobre sugerencias y reclamaciones.

3. Cada servicio de salud regulará los procedimientos y los sistemas para garantizar el efectivo cumplimiento de las previsiones de este artículo.

Artículo 13. Derecho a la información para la elección de médico y de centro

Los usuarios y pacientes del Sistema Nacional de Salud, tanto en la atención primaria como en la especializada, tendrán derecho a la información previa correspondiente para elegir médico, e igualmente centro, con arreglo a los términos y condiciones que establezcan los servicios de salud competentes.

CAPÍTULO V

La historia clínica

Artículo 14. Definición y archivo de la historia clínica

1. La historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro.

2. Cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información.

3. Las Administraciones sanitarias establecerán los mecanismos que garanticen la autenticidad del contenido de la historia clínica y de los cambios operados en ella, así como la posibilidad de su reproducción futura.

4. Las Comunidades Autónomas aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental.

Artículo 15. Contenido de la historia clínica de cada paciente

1. La historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. Todo paciente o usuario tiene derecho a que quede constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud tanto en el ámbito de atención primaria como de atención especializada.

2. La historia clínica tendrá como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud. El contenido mínimo de la historia clínica será el siguiente:

a) La documentación relativa a la hoja clínicoestadística.

b) La autorización de ingreso.

c) El informe de urgencia.

d) La anamnesis y la exploración física.

e) La evolución.

f) Las órdenes médicas.

g) La hoja de interconsulta.

h) Los informes de exploraciones complementarias. i) El consentimiento informado.

j) El informe de anestesia.

k) El informe de quirófano o de registro del parto. I) El informe de anatomía patológica.

m) La evolución y planificación de cuidados de enfermería.

n) La aplicación terapéutica de enfermería.

ñ) El gráfico de constantes.

o) El informe clínico de alta.

Los párrafos b), c), i), j), k), l), ñ) y o) sólo serán exigibles en la cumplimentación de la historia clínica cuando se trate de procesos de hospitalización o así se disponga.

3. La cumplimentación de la historia clínica, en los aspectos relacionados con la asistencia directa al paciente, será responsabilidad de los profesionales que intervengan en ella.

4. La historia clínica se llevará con criterios de unidad y de integración, en cada institución asistencial como mínimo, para facilitar el mejor y más oportuno conocimiento por los facultativos de los datos de un determinado paciente en cada proceso asistencial.

Artículo 16. Usos de la historia clínica

1. La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.

2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.

5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en

relación con los pacientes y usuarios o la propia Administración sanitaria.

6. El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto.

7. Las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso.

Artículo 17. La conservación de la documentación clínica

1. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial.

2. La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas.

3. Los profesionales sanitarios tienen el deber de cooperar en la creación y el mantenimiento de una documentación clínica ordenada y secuencia¡ del proceso asistencial de los pacientes.

4. La gestión de la historia clínica por los centros con pacientes hospitalizados, o por los que atiendan a un número suficiente de pacientes bajo cualquier otra modalidad asistencial, según el criterio de los servicios de salud, se realizará a través de la unidad de admisión y documentación clínica, encargada de integrar en un solo archivo las historias clínicas. La custodia de dichas historias clínicas estará bajo la responsabilidad de la dirección del centro sanitario.

5. Los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen.

6. Son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

Artículo 18. Derechos de acceso a la historia clínica

1. El paciente tiene el derecho de acceso, con las reservas señaladas en el apartado 3 de este artículo, a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella. Los centros sanitarios regularán el procedimiento que garantice la observancia de estos derechos.

2. El derecho de acceso del paciente ala historia clínica puede ejercerse también por representación debidamente acreditada.

3. El derecho al acceso del paciente ala documentación de la historia clínica no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas.

4. Los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. En cualquier caso el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que afecte ala intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros.

Artículo 19. Derechos relacionados con la custodia de la historia clínica

El paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad con arreglo a lo establecido por el artículo 16 de la presente Ley.

CAPÍTULO VI

Informe de alta y otra documentación clínica

Artículo 20. Informe de alta

Todo paciente, familiar o persona vinculada a él, en su caso, tendrá el derecho a recibir del centro o servicio sanitario, una vez finalizado el proceso asistencial, un informe de alta con los contenidos mínimos que determina el artículo 3. Las características, requisitos y condiciones de los informes de alta se determinarán reglamentariamente por las Administraciones sanitarias autonómicas.

Artículo 21. El alta del paciente

1. En caso de no aceptar el tratamiento prescrito, se propondrá al paciente o usuario la firma del alta voluntaria. Si no la firmara, la dirección del centro sanitario, a propuesta del médico responsable, podrá disponer el alta forzosa en las condiciones reguladas por la Ley. El hecho de no aceptar el tratamiento prescrito no dará lugar al alta forzosa cuando existan tratamientos alternativos, aunque tengan carácter paliativo, siempre que los preste el centro sanitario y el paciente acepte recibirlos. Estas circunstancias quedarán debidamente documentadas.

2. En el caso de que el paciente no acepte el alta, la dirección del centro, previa comprobación del informe clínico correspondiente, oirá al paciente y, si persiste en su negativa, lo pondrá en conocimiento del juez para que confirme o revoque la decisión.

Artículo 22. Emisión de certificados médicos

Todo paciente o usuario tiene derecho a que se le faciliten los certificados acreditativos de su estado de salud. Éstos serán gratuitos cuando así lo establezca una disposición legal o reglamentaria.

Artículo 23. Obligaciones profesionales de información técnica, estadística y administrativa

Los profesionales sanitarios, además de las obligaciones señaladas en materia de información clínica, tienen el deber de cumplimentar los protocolos, registros, informes, estadísticas y demás documentación asistencial o administrativa, que guarden relación con los procesos clínicos en los que intervienen, y los que requieran

los centros o servicios de salud competentes y las autoridades sanitarias, comprendidos los relacionados con la investigación médica y la información epidemiológica.

Disposición adicional primera. Carácter de legislación básica

Esta Ley tiene la condición de básica, de conformidad con lo establecido en el artículo 149.1.1.8 y 16.ª de la Constitución.

El Estado y las Comunidades Autónomas adoptarán, en el ámbito de sus respectivas competencias, las medidas necesarias para la efectividad de esta Ley.

Disposición adicional segunda. Aplicación supletoria

Las normas de esta Ley relativas a la información asistencial, la información para el ejercicio de la libertad de elección de médico y de centro, el consentimiento informado del paciente y la documentación clínica, serán de aplicación supletoria en los proyectos de investigación médica, en los procesos de extracción y trasplante de órganos, en los de aplicación de técnicas de reproducción humana asistida y en los que carezcan de regulación especial.

Disposición adicional tercera. Coordinación de las historias clínicas

El Ministerio de Sanidad y Consumo, en coordinación y con la colaboración de las Comunidades Autónomas competentes en la materia, promoverá, con la participación de todos los interesados, la implantación de un sistema de compatibilidad que, atendida la evolución y disponibilidad de los recursos técnicos, y la diversidad de sistemas y tipos de historias clínicas, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, en evitación de que los atendidos en diversos centros se sometan a exploraciones y procedimientos de innecesaria repetición.

Disposición adicional cuarta. Necesidades asociadas a la discapacidad

El Estado y las Comunidades Autónomas, dentro del ámbito de sus respectivas competencias, dictarán las disposiciones precisas para garantizar a los pacientes o usuarios con necesidades especiales, asociadas a la discapacidad, los derechos en materia de autonomía, información y documentación clínica regulados en esta Ley.

Disposición adicional quinta. Información y documentación sobre medicamentos y productos sanitarios

La información, la documentación y la publicidad relativas a los medicamentos y productos sanitarios, así como el régimen de las recetas y de las órdenes de prescripción correspondientes, se regularán por su normativa específica, sin perjuicio de la aplicación de las reglas establecidas en esta Ley en cuanto a la prescripción y uso de medicamentos o productos sanitarios durante los procesos asistenciales.

Disposición adicional sexta. Régimen sancionador

Las infracciones de lo dispuesto por la presente Ley quedan sometidas al régimen sancionador previsto en el capítulo VI del Título I de la Ley 14/1986, General de Sanidad, sin perjuicio de la responsabilidad civil o penal y de la responsabilidad profesional o estatutaria procedentes en derecho.

Disposición transitoria única. Informe de alta

El informe de alta se regirá por lo dispuesto en la Orden del Ministerio de Sanidad, de 6 de septiembre de 1984, mientras no se desarrolle legalmente lo dispuesto en el artículo 20 de esta Ley.

Disposición derogatoria única. Derogación general y de preceptos concretos

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en la presente Ley y, concretamente, los apartados 5, 6, 8, 9 y 11 del artículo 10, el apartado 4 del artículo 11 y el artículo 61 de la Ley 14/1986, General de Sanidad.

Disposición final única. Entrada en vigor

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

Por tanto,

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

Madrid, 14 de noviembre de 2002.

JUAN CARLOS R.

El Presidente del Gobierno,

JOSÉ MARÍA AZNAR LÓPEZ

Osakidetza

ACUERDO de 19 de Junio de 2006,

del Consejo de Administración del Ente Público Osakidetza, por el que se regulan los ficheros de carácter personal gestionados por Osakidetza

Septiembre 2007

Xedapen Orokorrak

OSASUN SAILA

6484

ERABAKIA, 2006ko ekainaren 19koa, Osakidetza-Euskal Osasun Zerbitzua Ente Publikoaren Administrazio Kontseiluarena, Osakidetza-Euskal Osasun Zerbitzuak kudeatutako datu pertsonalak dauzkaten fitxategiak arautzen dituena.

Osakidetzako Administrazio Kontseiluak 2001eko uztailaren 21ean eta 2004ko maiatzaren 13an hartutako erabakien bitartez arautu egin ziren erakunde publiko horren izaera pertsonaleko fitxategiak. Xedapen horiek Izaera Pertsonaleko Datuak Babesteko abenduaren 13ko 15/1999 Lege Organikoaren babespean eman ziren.

Aipatu 15/1999 Lege Organikoak 20.1 artikuluan ezarritakoaren arabera, herri-administrazioen fitxategiak sortu, aldatu edo ezabatzeko xedapen orokorra eman behar da eta Estatuko Aldizkari Ofizialean edo behar den aldizkari ofizialean argitaratu behar da. Artikulu bereko 3. paragrafoak adierazten du fitxategiak deuseztatzeko ematen diren xedapenetan berauen helburua ezarri behar dela edo, dagokion kasuan, suntsipenerako hartzen diren neurriak zehaztu behar direla.

Bestalde, Datuak Babesteko Agentziaren estatutuak onartzen dituen martxoaren 26ko 428/1993 Errege Dekretuko 24.1.e) artikuluak xedatzen duenaren arabera, autonomia erkidegoetako administrazioaren eta haren menpeko erakunde eta organoen jabetzako fitxategi automatizatuak Datuak Babesteko Erregistro Nagusian erroldatuko dira.

Eusko Legebiltzarraren otsailaren 25eko 2/2004 Legeak, Jabetza Publikoko Datu Pertsonalen Fitxategiei eta Datuen Babeserako Euskal Agentziari buruzkoak, bere 4.2 artikuluan, honako hau ezartzen du: «Datu pertsonalen fitxategiak beste administrazio, erakunde edo korporazio batzuetakoak badira, berriz, horiek sortu, aldatu edo ezabatzeko erabakiak edo xedapenak derrigorrezko aipamen guztiak jaso beharko ditu eta Euskal Herriko Agintaritzaren Aldizkarian edo lurralde historikoko aldizkarian argitaratuko da, fitxategia duenaren eginkizun edo aginpideak zein lurralde-eremutara iristen diren kontuan hartuta».

2/2004 Lege horrek, bere lehenengo xedapen gehigarrian zehazten duenez, bere eremura lotuak dauden administrazio publiko, erakunde eta korporazioek euren jabetzako izaera pertsonaleko datuen fitxategien

Disposiciones Generales

DEPARTAMENTO DE SANIDAD

6484

ACUERDO de 19 de junio de 2006, del Consejo de Administración del Ente Público Osakidetza-Servicio vasco de salud, por el que se regulan los ficheros de carácter personal gestionados por Osakidetza-Servicio vasco de salud.

Por medio de los Acuerdos del Consejo de Administración de Osakidetza–Servicio vasco de salud de 21 de julio de 2001 y de 13 de mayo de 2004, se procedió a la regularización de los ficheros de carácter personal del citado Ente Público. Tales disposiciones fueron dictadas al amparo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Dicha norma, establece en su artículo 20.1, que la creación, modificación o supresión de los ficheros de las Administraciones Públicas deberá hacerse mediante disposición general publicada en Boletín Oficial del Estado o diario oficial correspondiente. En el apartado 3 del mismo artículo, se señala que 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.

Por otra parte, el artículo 24.1.e) del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, dispone que serán objeto de inscripción, en el Registro General de Protección de Datos, los ficheros automatizados que contengan datos personales y de los cuales sean titulares las Administraciones de las Comunidades Autónomas, así como sus entes y organismos dependientes.

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 determina en su artículo 4.2 que 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.

Asimismo, la Ley mencionada en el párrafo anterior, en su Disposición Adicional Primera, estipula que las Administraciones públicas, instituciones y corporaciones sujetas al ámbito de esta Ley comunicarán a la Agen-

berri eman behar diote Datuak Babeseko Euskal Bulegoari, legea indarrean jarri eta hiru hilabeteko epean. Hori baino lehenago, kasuan kasuko fitxategia arautzeko xedapena onarturik eta argitaraturik izan behar dute.

Beste fitxategi automatizatu batzuk gehitzeko beharra sortu da, eta fitxategi horien edukia aipaturiko 15/1999 Lege Organikoan aurreikusitakora egokitu behar da. Hortaz, Osakidetzako izaera pertsonaleko datu-fitxategien berri herritarrek izan dezaten, erabaki honetan biltzen dira izaera pertsonaleko datu-fitxategi guztiak. Erabaki honen bidez indargabetu egiten dira izaera pertsonaleko datu-fitxategiak arautzen dituzten xedapen guztiak, ezabatu egiten ditu orain arteko fitxategiak eta txertatu egiten ditu orain arteko xedapenek araututako fitxategiak, xedapenek edo denbora igarotzeak gomendagarri egiten dituzten aldaketak eta egokitzapenak sartuz. Beraz, fitxategiak hainbat xedapenetan ez sakabanatzeko, eta herritarren argitasun eta segurtasun juridikoaren mesedetan, Kultura Saileko eta Helduen Alfabetatze eta Berreuskalduntzerako Erakundeko datu pertsonalen fitxategi guztiak zerrendatu dira xedapen honen II. eta III. eranskinetan. Eranskin horietan, gainera, aurreko xedapenetan azaltzen ez ziren fitxategi berri batzuk ere sartu dira. I. eranskinean erabaki honek ezabatzen dituen Osakidetzako fitxategiak jasotzen dira.

Euskadiko Antolamendu Sanitarioaren 8/1997 Legeak berezko izaera juridikoa eta zerbitzu sanitarioak emateko zereginean jarduteko gaitasun osoa aitortzen dio Osakidetza-Euskal Osasun Zerbitzuari. Beraz, Administrazio Kontseilu honen eskumena da Osakidetza-Euskal Osasun Zerbitzuaren jabetzako datu pertsonalen fitxategi automatizatuak arautu eta kudeatzea.

Ondorioz, legezko xedapenek eman dizkidaten eskumenez baliatuz, hauxe

ERABAKIA:

Lehenengoa.– Xedea.

1.– Osakidetza-Euskal Osasun Zerbitzuak kudeatzen dituen izaera pertsonaleko datu-fitxategi berriak arautzea; fitxategi horiek 15/1999 Lege Organikoaren ezarpen-eremukoak dira eta erabaki honetako II. eta III. eranskinetan jasota eta deskribatuta daude. I. eranskinean jasotakoak ezabatzea ere onartzen da.

2.– Datu pertsonalak babesteko abenduaren 13ko 15/1999 Lege Organikoak bere 20.2. artikuluan dioenari jarraiki, agindu honen eranskinetan azaltzen diren datu pertsonalen fitxategietako bakoitzak honakoak jasoko ditu: fitxategien helburuak eta berauentzat aurreikusten diren erabilpenak, zein pertsona edo talderengandik lortu nahi diren datu pertsonalak edo zein dauden datuok ematera behartuak, datuok jasotzeko prozedurak, fitxategien oinarrizko egiturak, barne hartzen dituzten datu-motak adierazita, datuentzat aurreicia 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 que sean de su titularidad, previa aprobación y publicación de la disposición reguladora correspondiente.

Habiendo surgido la necesidad de incorporar nuevos ficheros y adecuar los existentes en base al contenido de lo previsto en la citada Ley Orgánica 15/1999, y al fin de facilitar el conocimiento público de los ficheros de datos de carácter personal de Osakidetza – Servicio vasco de salud, se aúnan todos los ficheros de datos de carácter personal en el presente Acuerdo, que deroga las anteriores disposiciones reguladoras de ficheros de datos de carácter personal, suprimiendo todos los ficheros preexistentes e incorporando los ficheros ya regulados por éstas, con las modificaciones y adecuaciones que las disposiciones o el transcurso del tiempo recomiendan. Con el propósito de no disgregar los ficheros en distintas disposiciones, y siempre en aras a la claridad y seguridad jurídica de los ciudadanos, se enumeran todos los ficheros de datos de carácter personal de Osakidetza – Servicio vasco de salud en los anexos II y III de la presente disposición, en el que además, se incluyen otros nuevos ficheros que no aparecían en las anteriores disposiciones. Asimismo, en el anexo I se enumeran los ficheros de Osakidetza – Servicio vasco de salud suprimidos por el presente Acuerdo.

Toda vez que la Ley 8/1997 de Ordenación sanitaria de Euskadi otorga al Ente Público personalidad jurídica propia y plena capacidad de obrar en su función de provisor de servicios sanitarios, es competencia de este Consejo de Administración la regulación y gestión de los ficheros de datos de carácter personal existentes en el Ente Público.

En su virtud, de conformidad con las facultades otorgadas por las disposiciones legales,

ACUERDO:

Primero.– Objeto.

1.– Aprobar la regulación de los nuevos ficheros de datos de carácter personal gestionados por el Ente Público Osakidetza-Servicio vasco de salud, incluidos en el ámbito de aplicación de la Ley Orgánica 15/1999, que se relacionan y describen en los anexos II y III de este acuerdo, así como la supresión de los incluidos en el anexo I.

2.– De conformidad con el artículo 20.2 de la citada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se indicará para cada uno de los ficheros de datos de carácter personal mencionados en los anexos a la presente Orden: las finalidades de los ficheros y los usos previstos para los mismos, las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos, los procedimientos de recogida de los mismos, las estructuras básicas de los fiche-

kusiriko lagapen edota nazioarteko transferentziak, fitxategien ardura dagokien Administrazioko organoak, datuak eskuratu, zuzendu, deuseztatu edo aurkatzeko eskubideak zein zerbitzu edo unitatetan erabil daitezkeen, eta fitxategietako bakoitzari ezarri ahal izango zaizkion segurtasun-neurrien mailaren adierazpena (oinarrizkoa, ertaina, jasoa).

Bigarrena.– Neurriak hartzea.

Fitxategi automatizatu bakoitzaren organo arduradunen titularrek beharrezkoak diren neurriak hartuko dituzte datuen konfidentzialtasuna, segurtasuna eta osotasuna ziurta daitezen, eta 15/1999 Lege Organikoan eta indarrean dauden gainontzeko xedapenetan aitortutako gainerako bermeak, betebeharrak eta eskubideak gauza daitezen.

Hirugarrena.– Fitxategien helburua eta datuak uztea.

1.– Erabaki honetako fitxategien helburuak eranskinean daude jasota. Hala ere, helburu horietaz gain, beste hauek ere izango dituzte: azterketa epidemiologikoak eta osasun ikerketak egitea. Azkenik, estatistikak egiteko ere erabili ahal izango dira.

2.– Era berean, Euskal Autonomia Erkidegoko Administrazio Publikoko eta beste administrazio publiko batzuetako estatistika-organo eta -zerbitzuei laga ahal izango zaizkie, kontuan edukiz Euskal Autonomia Erkidegoko Estatistikari buruzko apirilaren 23ko 4/1986 Legean eta Funtzio Estatistiko Publikoari buruzko maiatzaren 9ko 12/1989 Legean ezartzen dena. Osasun eremuari dagokionean, Osasun Sailari utzi ahal izango zaizkio datuen babesaren gaineko indarreango arauetan ezarritako moduan, baita beste sail edo erakunde publiko batzuei ere, ikerketa eta estatistiken eremuan lege-ordenamenduak agindutako zereginak betetzeko.

Laugarrena.– Datuen tratamendu-zerbitzua ematea.

Datu-tratamenduaren arduradunak emandako jarraibideak kontuan hartu beharko dituzte Kultura Sailaren eta Helduen Alfabetatze eta Berreuskalduntzerako Erakundearen (HABE) kontura datu pertsonalen tratamendu-zerbitzua ematen dutenek, eta jarraibide horien arabera jardungo dute. Hala egingo dutela jasoko da zerbitzua eskaintzeko egiten den kontratuan. Beraz, alde batetik, datuak ezin izango dira beste ezertarako aplikatu edo erabili, eta bestetik, ezin izango zaio inori haien berri eman, nahiz eta asmoa datuak gordetzea izan; izan ere, hala agintzen du abenduaren 13ko 15/1999 Lege Organikoaren 12. artikuluak.

Bosgarrena.– Datuen aurka egiteko nahiz datuak ikusi, zuzendu edo deuseztatzeko eskubidea.

ros, indicando los tipos de datos que incluyen, las cesiones de datos y/o transferencias internacionales previstas, los órganos de la Administración responsables de los ficheros, los servicios o unidades ante los que podrán ejercitarse los derechos de acceso, rectificación, cancelación y oposición, y la indicación del nivel (básico, medio, alto) de las medidas de seguridad aplicables a cada uno de ellos.

Segundo.– Adopción de medidas.

Los titulares de los órganos responsables de cada fichero adoptarán las medidas necesarias para asegurar la confidencialidad, seguridad e integridad de los datos, así como las conducentes a hacer efectivas las demás garantías, obligaciones y derechos reconocidos en la citada Ley Orgánica 15/1999 y en las demás normas vigentes.

Tercero.– Finalidad de los ficheros y cesiones de datos.

1.– Los ficheros objeto del presente Acuerdo, además de servir a los fines que para cada uno se indican en el correspondiente anexo, tendrán como objetivo la realización de estudios epidemiológicos y la investigación sanitaria. Asimismo, tendrán como finalidad su utilización estadística.

2.– Los datos contenidos en dichos ficheros podrán ser cedidos a los órganos y servicios de estadística de la Administración Pública de la Comunidad Autónoma de Euskadi y de otras Administraciones Públicas, al amparo de lo dispuesto en la Ley 4/1986, de 23 de abril, de Estadística de la Comunidad Autónoma de Euskadi y en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública. En el ámbito sanitario asimismo, podrán ser cedidos al Departamento de Sanidad, en los términos contemplados en la normativa vigente relativa a la protección de datos, así como a otros departamentos u organismos públicos para desarrollar labores de investigación y estadística, en el cumplimiento de las funciones encomendadas por el ordenamiento jurídico.

Cuarto.– Prestación de servicios de tratamiento de datos.

Quienes, por cuenta de Osakidetza – Servicio vasco de salud, presten servicios de tratamiento de datos de carácter personal realizarán las funciones encomendadas conforme a las instrucciones del responsable del tratamiento y así se hará constar en el contrato que a tal fin se celebre, no pudiendo aplicarlos o utilizarlos con fin distinto, ni comunicarlos, ni siquiera para su conservación, a otras persona, de conformidad con lo dispuesto en el artículo 12 de la mencionada Ley Orgánica 15/1999.

Quinto.– Derecho de oposición, acceso rectificación y cancelación de datos.

Fitxategietan agertzen direnek eskubidea dute datuen aurka egiteko nahiz datuak ikusi, zuzendu edo deuseztatzeko. Beraz, bidezko denean, eskubide hori erabili ahal izango dute, eta horretarako, fitxategi bakoitzerako erabaki honen eranskinean zehazten den unitatera edo zerbitzura jo beharko dute.

Seigarrena.– Fitxategien arduraduna.

Osakidetzak kudeatutako fitxategien arduradun izateko nahitaezkoa izango da erabaki honetako dagokion eranskinean arduradun legetxe azaltzea.

Zazpigarrena.– Datuak Babesteko Erregistro Nagusian fitxategiak erregistratzea.

Datuak Babesteko Agentziari jakinaraziko zaizkio erabaki honetan zerrendatutako fitxategiak, honek fitxategiak ezaba ditzan eta Datuak Babesteko Erregistro Nagusian sar ditzan. Horretarako, xedapen honen kopia bat bidaliko da Agentziara, eta kopia bidaltzeko, Agentziak egindako eredu normalizatua erabiliko da.

Zortzigarrena.– EHAAn argitaratzea.

Agindu hau indarrean jartzen denean, indargabetuta gelditukо dira bertan ezarritakoaren aurka doazen maila bereko edo beheragoko xedapen guztiak, eta bereziki honako hauek:

a) Erabakia, 2001eko irailaren 26koa, Osakidetza-Euskal Osasun Zerbitzua Ente Publikoaren Administrazio Kontseiluarena, Osakidetza-Euskal Osasun Zerbitzuak kudeatutako datu pertsonalak dauzkaten fitxategiak arautzen dituena.

b) Erabakia, 2004ko maiatzaren 13koa, Osakide-tza-Euskal Osasun Zerbitzua Ente Publikoaren Administrazio Kontseiluarena, Osakidetza-Euskal Osasun Zerbitzuak kudeatutako datu pertsonalak dauzkaten fitxategiak arautzen dituena.

Erabaki honek Euskal Herriko Agintaritzaren Aldizkarian argitaratzen den egunaren biharamunean izango du eragina.

Vitoria-Gasteiz, 2006ko ekainaren 19a.

Osakidetza-Euskal Osasun Zerbitzuko
Administrazio Kon-tseiluko lehendakaria,
GABRIEL M.ª INCLÁN IRIBAR.

Ale Gehigarri bereizian argitaratzen dira aipaturiko eranskinak

Los afectados de los ficheros podrán ejercitar su derecho de oposición, acceso, rectificación y cancelación de datos, cuando proceda, ante la Unidad o Servicio que para cada fichero se determine en el anexo correspondiente de este Acuerdo.

Sexto.– Responsable de los ficheros.

Serán responsables de los ficheros gestionados por Osakidetza – Servicio vasco de salud los que con tal carácter figuren en el anexo correspondiente del presente Acuerdo.

Séptimo.– Inscripción de los ficheros en el Registro de Protección de Datos.

Los ficheros relacionados en este Acuerdo serán notificados a la Agencia Vasca de Protección de Datos para su correspondiente supresión e inscripción en el Registro de Protección de Datos, mediante el traslado, a través del modelo normalizado elaborado a tal efecto por la Agencia, de una copia de la presente disposición.

Octavo.– Publicación en boletín.

A la publicación en el BOPV del presente Acuerdo, quedarán sin efecto cuantas disposiciones de igual o inferior rango se opongan a lo establecido en el mismo, y en particular las siguientes:

a) Acuerdo de 26 de septiembre de 2001, del Consejo de Administración del Ente Público Osakidetza-Servicio vasco de salud, por el que se regulan los ficheros automatizados de datos de carácter personal gestionados por Osakidetza-Servicio vasco de salud.

b) Acuerdo de 13 de mayo de 2004, del Consejo de Administración del Ente Público Osakidetza-Servicio vasco de salud, por el que se regulan los ficheros automatizados de datos de carácter personal gestionados por Osakidetza-Servicio vasco de salud.

Este Acuerdo surtirá efectos el día siguiente al de su publicación en el Boletín Oficial del País Vasco.

En Vitoria–Gasteiz, a 19 de junio de 2006.

El Presidente del Consejo de Administración
de Osakidetza-Servicio vasco de salud,
GABRIEL M.ª INCLÁN IRIBAR.

En Suplemento aparte se publican los anexos que se citan

Osakidetza

ACUERDO de 24 de Enero de 2007,

del Consejo de Administración de Osakidetza, por el que se modifica la estructura de la Comisión de Seguridad para la Protección de Datos de Osakidetza

Septiembre 2007

Bigarrena.– Dekretu honek administrazio-bidea agortzen du; haren aurka, administrazioarekiko auzierrekurtsoa jar daiteke EAEko Auzitegi Nagusian, bi hilabeteko epean, Euskal Herriko Agintaritzaren Aldizkarian argitaratu eta hurrengo egunetik kontatzen hasita, Administrazioarekiko Auzien Jurisdikzioa arautzen duen uztailaren 13ko 29/1998 Legearen 10.1.b) eta 46.1. artikuluetan ezarritakoaren arabera.

Hirugarrena.– Euskal Herriko Agintaritzaren Aldizkarian argitaratzen den egunaren biharamunean jarriko da indarrean dekretu hau.

Vitoria-Gasteizen, 2007ko otsailaren 27an.

Lehendakaria,
JUAN JOSÉ IBARRETXE MARKUARTU.

Etxebizitza eta Gizarte Gaietako sailburua,
JAVIER MADRAZO LAVÍN.

Segunda.– Contra el presente Decreto, que agota la vía administrativa, las personas interesadas podrán interponer recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia del País Vasco en el plazo de dos meses contados desde el día siguiente al de su publicación en el mismo diario oficial, conforme a lo establecido en los artículos 10.1.b) y 46.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa.

Tercera.– El presente Decreto entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del País Vasco.

Dado en Vitoria-Gasteiz, a 27 de febrero de 2007.

El Lehendakari,
JUAN JOSÉ IBARRETXE MARKUARTU.

El Consejero de Vivienda y Asuntos Sociales,
JAVIER MADRAZO LAVÍN.

OSASUN SAILA

1589

ERABAKIA, 2007ko urtarrilaren 24koa, Osakidetza-Euskal Osasun Zerbitzuaren Administrazio Kontseiluarena, Osakidetza-Euskal Osasun Zerbitzuaren datuak babesteko Segurtasun Batzordearen egitura aldatzen duena.

2003ko martxoaren 28an eman zen Osakidetza-Euskal Osasun Zerbitzua ente publikoaren Administrazioko Kontseiluaren erabakia, Osakidetza-Euskal Osasun Zerbitzuaren datuak babesteko Segurtasun Batzordea sortu eta haren zereginak ezartzekoa.

Denbora luzea pasa da sortu zenetik eta hasieran izan zuen egituran hainbat arlo korporatibo sartzeko beharra ikusi da, jardueren hasieran eman nahi izan zitzaion izaera nagusiki sanitarioa eta informatikoa zenez, bere garaian kanpoan geratu baitziren. Hala ere, ikusirik datuen babesean Osakidetza-Euskal Osasun Zerbitzuan lortutako esperientzia positiboa, komeni da segurtasuneko batzorde hori zabaltzea, aipatu den bezala.

Horregatik jotzen da bidezkoa egitura horren barruan zerbitzu zentralen antolaketan dauden segmentu guztiak sartzea.

Eta, horrenbestez, azaldutakoaren arabera, Administrazio Batzorde honek honako hau erabaki du, azal-

DEPARTAMENTO DE SANIDAD

1589

ACUERDO de 24 de enero de 2007, del Consejo de Administración de Osakidetza-Servicio vasco de salud, por el que se modifica la estructura de la Comisión de Seguridad para la Protección de Datos de Osakidetza-Servicio vasco de salud.

Con fecha 28 de marzo de 2003, se dictó Acuerdo del Consejo de Administración del ente público Osakidetza-Servicio vasco de salud, por el que se procedía a crear y a asignar funciones a la denominada «Comisión de Seguridad para la Protección de Datos de Osakidetza-Servicio vasco de salud».

Habiendo transcurrido un largo periodo de tiempo desde su creación, se manifiesta la necesidad de incorporar en su estructura inicial, determinadas áreas corporativas que en su momento quedaron fuera de la misma, dado el carácter preeminentemente sanitario e informático que se le quiso imprimir en el inicio de sus actividades. No obstante, a la vista de la experiencia positiva obtenida en Osakidetza-Servicio vasco de salud en el campo de la protección de datos, resulta aconsejable la ampliación de dicha comisión de seguridad, en los términos ya mencionados.

Es por ello, que se considera oportuno incluir dentro de dicha estructura, a la totalidad de segmentos presentes en la organización de servicios centrales.

Y, por tanto, de conformidad con la exposición que antecede, este Consejo de Administración, para debido

dutakoa behar bezala betetzeko eta aipatutako estatutuen 8.5. artikuluak esleitzen dizkion eskumenen indarrez:

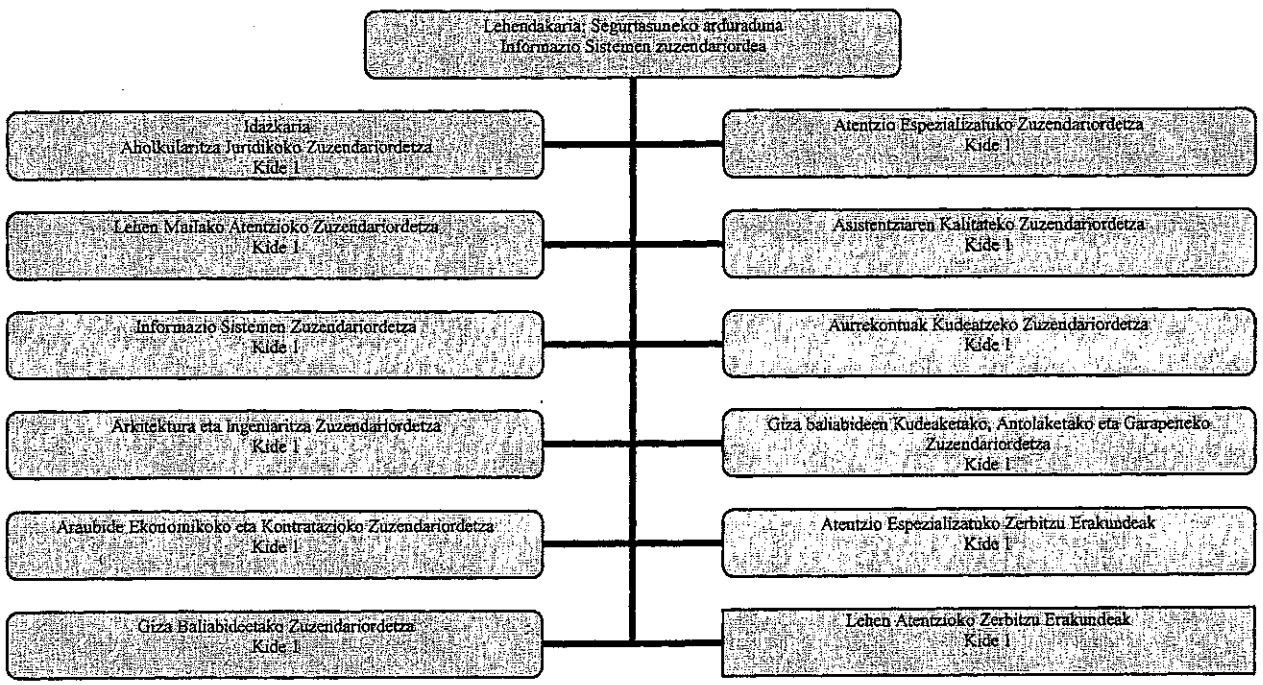
ERABAKIA:

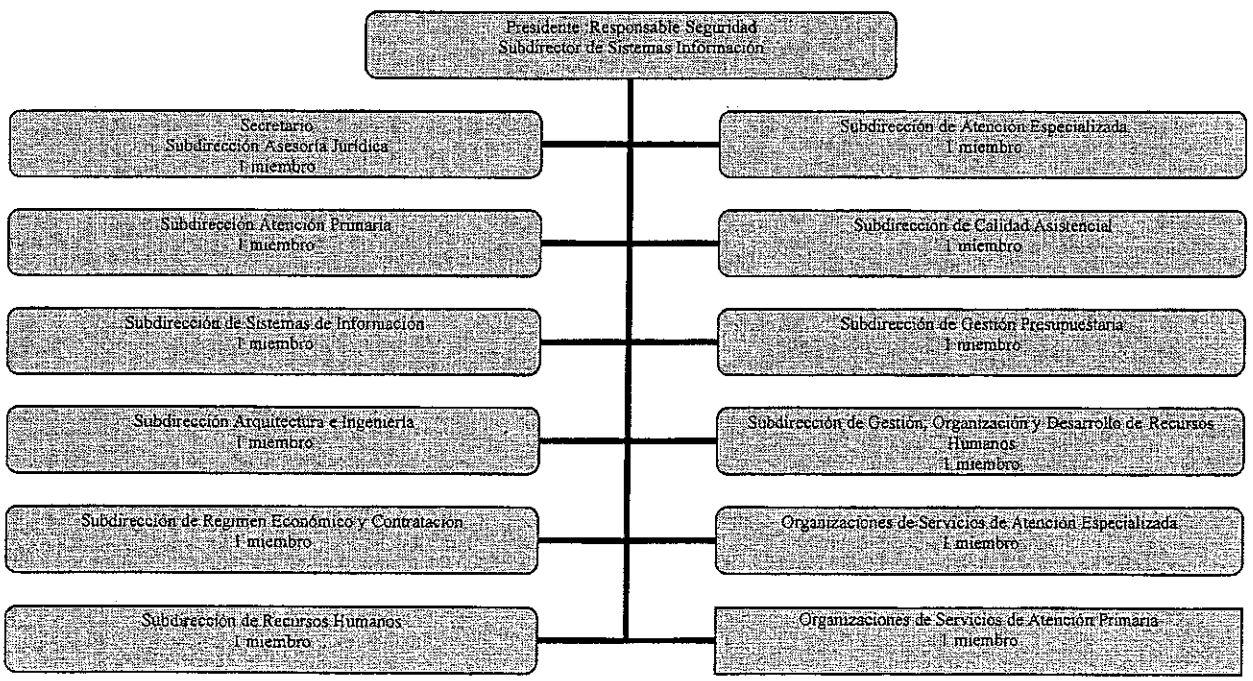
Lehenengoa.– Osakidetza-Euskal Osasun Zerbitzuaren datuak babesteko Segurtasun Batzordearen organigrama aldatzea. Aurrerantzean honelakoa izango da:

cumplimiento de lo expuesto y en virtud de las competencias atribuidas al mismo en el artículo 8.5 de los referidos Estatutos Sociales, viene a adoptar el siguiente

ACUERDO:

Primero.– Modificar el organigrama de la comisión de seguridad para la protección de datos en Osakidetza-Servicio vasco de salud, que de ahora en adelante será el siguiente:





Erabaki honek hartzen egunetik izango ditu eraginak, Euskal Herriko Agintaritzaren Aldizkarian argitaratu nahiz ez, eta batzorderako izendatutako kideei jakinarazpena egin nahiz ez.

Vitoria-Gasteiz, 2007ko urtarrilaren 24a.

Administrazio Kontseiluko lehendakaria,
GABRIEL M.ª INCLÁN IRIBAR.

El presente acuerdo surtirá efectos a partir de la fecha de su adopción, sin perjuicio de su publicación en el Boletín Oficial del País Vasco y notificación personal a los miembros designados para la Comisión.

En Vitoria–Gasteiz, a 24 de enero de 2007.

El Presidente del Consejo de Administración,
GABRIEL M.ª INCLÁN IRIBAR.

Agintariak eta Langileria

Izendapenak, Egoerak eta Gorabeherak

HERRIZAINGO SAILA

1590

AGINDUA, 2007ko otsailaren 7koa, Herrizaingo sailburuarena, Luis Fernando Lekue Villar jaunak Herrizaingo Saileko Joko eta Ikuskizun Zuzendaritzako goi-kargudunaren idazkari izateari utz diezaiola xedatzen duena.

Euskal Funtzio Publikoari buruzko uztailaren 6ko 6/1989 Legearen 50.2 artikuluan xedatutakoarekin bat, eta lege horrek ematen dizkidan eskumenez baliatuz, honako hau

XEDATU DUT:

Lehenengoa.– Luis Fernando Lekue Villar jaunak, berak hala eskatuta, Herrizaingo Saileko Joko eta Ikuskizun Zuzendaritzako goi-kargudunaren idazkari izateari utz diezaiola, egindako lanagatik eskerrak emanez. Lanpostua: kodea 1001, dotazioa 57, 18. maila.

Bigarrena.– Kargu-uzte honek 2007ko otsailaren 12tik aurrera izango ditu ondorio ekonomikoak eta administratiboak.

Hirugarrena.– Agindu honek administrazio-bidea agortzen du, eta bere aurka berraztertzeko errekurtsoa aurkeztu ahal zaio agindua eman duen organoari, hilabeteko epean, jakinarazpena egiten den egunetik hasita; edo, bestela, administrazioarekiko auzi-errekurtsoa aurkez daiteke Administrazioarekiko Auzietako Epaitegian, bi hilabeteko epean, agindua EHAAn argitaratu eta hurrengo egunetik hasita.

Vitoria-Gasteiz, 2007ko otsailaren 7a.

Herrizaingo sailburua,
JAVIER BALZA AGUILERA.

Autoridades y Personal

Nombramientos, Situaciones e Incidencias

DEPARTAMENTO DE INTERIOR

1590

ORDEN de 7 de febrero de 2007, del Consejero de Interior, por la que se dispone el cese de D. Luis Fernando Lekue Villar como Secretario de Alto Cargo de la Dirección de Juego y Espectáculos del Departamento de Interior.

De conformidad con lo dispuesto en el artículo 50.2 de la Ley 6/1989, de 6 de julio, de la Función Pública Vasca y en uso de las atribuciones conferidas por esta misma Ley,

DISPONGO:

Primero.– Cesar, a petición propia, como Secretario de Alto Cargo de la Dirección de Juego y Espectáculos del Departamento de Interior, código 1001 dotación 57, nivel 18, a D. Luis Fernando Lekue Villar, agradeciéndole los servicios prestados.

Segundo.– Este cese producirá efectos económicos y administrativos el día 12 de febrero de 2007.

Tercero.– Contra la presente Orden, que agota la vía administrativa, podrá interponerse recurso potestativo de reposición ante el mismo órgano que lo hubiere dictado en el plazo de un mes a partir del día siguiente al de la notificación o recurso contencioso-administrativo ante el Juzgado de lo Contencioso-Administrativo de Vitoria-Gasteiz, en el plazo de dos meses a contar desde el día siguiente al de la publicación de la presente Orden en el Boletín Oficial del País Vasco.

En Vitoria-Gasteiz, a 7 de febrero de 2007.

El Consejero de Interior,
JAVIER BALZA AGUILERA.

Osakidetza

Instrucción Nº 2/2003 – Dirección General.

Asunto:

Modelo organizativo de seguridad para las organizaciones de servicios de Osakidetza

Septiembre 2007

INSTRUCCIÓN Nº 2/2003

DE: DIRECTOR GENERAL

A: DIRECTORES GERENTES DE ORGANIZACIONES DE SERVICIOS

ASUNTO: MODELO ORGANIZATIVO DE SEGURIDAD PARA LAS ORGANIZACIONES DE SERVICIOS DE OSAKIDETZA-SERVICIO VASCO DE SALUD

La Ley Orgánica 15/1999, de 13 de diciembre, relativa a la Protección de Datos de Carácter Personal, es de aplicación a los datos de carácter personal registrados en cualquier soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de los mismos. Define los **"datos de carácter personal"** como cualquier información concerniente a personas físicas identificadas o identificables y el **"tratamiento de datos"** como las 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.

Los datos personales relativos a la salud están especialmente protegidos, y respecto a ellos, la **Ley orgánica 15/1999** en su **artículo 8**, dice *"las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de 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 y autonómica sobre Sanidad".*

Mediante el Acuerdo del Consejo de Administración, de fecha 28 de marzo, se constituye la Comisión de Seguridad para la protección de los datos de carácter personal del Ente Público Osakidetza-Servicio vasco de salud.

Dicha Comisión de Seguridad se establece como máximo órgano consultivo y de apoyo a las diversas direcciones y subdirecciones de la organización, en la toma de las decisiones referidas a la seguridad de la información.

En el ejercicio de sus competencias, esta Comisión actúa por delegación y con el respaldo manifiesto de la Dirección General, máxima representación del Ente Público en su calidad de Responsable de los Ficheros que contengan datos de carácter personal, así como de las diversas Direcciones a las que se adscriben dichos ficheros, en su calidad de órganos internos responsables de los mismos.

Entre sus funciones, destacan las de definir las estrategias de seguridad, articular las normativas correspondientes a dicha materia, así como coordinar la ejecución de las acciones pertinentes, junto con el Responsable de Seguridad, a quien se atribuye en el Documento de Seguridad de Osakidetza-Servicio vasco de salud, entre otras misiones, el control y la supervisión de dichas actividades.

Osakidetza-Servicio vasco de salud, persona con entidad jurídica propia, se erige como Responsable último de todos los ficheros automatizados que contengan Datos de Carácter Personal en sus instalaciones.

La realización de una parte de las tareas operativas relacionadas con la seguridad que corresponden al Responsable de los Ficheros se delega en el Responsable de Seguridad, y el resto en los Responsables de Autorización de Accesos. Esta delegación de actividades no supone en ningún caso una exoneración de las responsabilidades, que en materia de seguridad de Datos de Carácter Personal corresponden legalmente a Osakidetza-Servicio vasco de salud.

De acuerdo con lo anterior, la Comisión de Seguridad decide en su momento, que por la Dirección General de Osakidetza-Servicio vasco de salud se emita la presente Instrucción, al objeto de articular debidamente el modelo organizativo descrito en el Documento de Seguridad del Ente Público para sus diversas organizaciones de servicios, facilitando así, con la creación de la infraestructura organizativa requerida, la puesta en marcha de la implantación de las medidas de seguridad exigidas por la legislación vigente en la materia, y por lo tanto, en virtud de las competencias atribuidas, en materia de coordinación y control, al Director General de esta Organización Administrativa Central, en el artículo 11 del Decreto 255/1997, se viene a establecer la siguiente

INSTRUCCION

Primero - Ámbito de aplicación y Objeto

La presente Instrucción será de aplicación en todas las organizaciones de servicios del Ente Público, siendo su objeto inmediato, el nombramiento de las figuras de Responsables de Seguridad y de Responsables de Autorización de Accesos en cada una de las organizaciones de servicios pertenecientes a Osakidetza-Servicio vasco de salud.

Estas figuras vienen enmarcadas dentro de la estructura organizativa de seguridad prevista en Osakidetza-Servicio vasco de salud, y les corresponden las funciones previstas en el Documento de Seguridad creado al efecto y que se describen en los artículos Quinto y Sexto de la presente Instrucción.

Dichos nombramientos deberán llevarse a cabo por los Gerentes de las diferentes organizaciones de servicios, encargados de coordinar y supervisar las tareas a realizar por dichos responsables, en virtud de lo dispuesto en el artículo 15 del decreto 255/1997, de 11 de Noviembre, por el que se establecen los Estatutos Sociales del Ente Público Osakidetza-Servicio vasco de salud.

Segundo - Criterios

La Comisión de Seguridad, en el ejercicio de sus funciones, ha determinado que dichos nombramientos han de seguir los siguientes criterios:

- Los Gerentes de las organizaciones de servicios, los cuales se erigen como responsables y coordinadores últimos en el ámbito de su propio centro, deberán designar como Responsables de Accesos a las personas encargadas de gestionar los servicios involucrados en las Direcciones y Subdirecciones de las diferentes áreas de cada organización de servicios (Dirección Médica, Dirección de Enfermería, Dirección de RR.HH., Dirección Económico- Financiera, etc.). En función de las dimensiones y la complejidad organizativa de cada caso concreto, las Gerencias y las Direcciones o Subdirecciones, determinarán la necesidad de atribuir esta responsabilidad a las Jefaturas de Servicios correspondientes. De forma general, es válido que esta responsabilidad se atribuya a la Dirección o Subdirección propietaria del proceso en que se manejan los datos personales (por ejemplo, en cuanto se refiera a la gestión del personal, nóminas, etc. de la organización la figura Responsable de Autorización de Accesos será la Dirección de RR.HH).

- Como Responsables de Seguridad se dispone que lo sean las Direcciones / Subdirecciones / Responsables de Informática de las organizaciones de servicios, considerando el contenido del Acuerdo del Consejo de Gobierno, de 16 de julio de 2002, sobre la organización de la seguridad de los ficheros automatizados de datos de carácter personal de la Administración de la CAPV, en cuya exposición de motivos se establece la conveniencia de que el Responsable de Seguridad sea un experto informático.

Tercero - Excepciones

En ausencia de Direcciones / Subdirecciones / Responsables de Informática, el Responsable de Autorización de Accesos de mayor rango asumirá las funciones del Responsable de Seguridad.

Se apunta que esta situación se produce actualmente en las siguientes organizaciones de servicios:

- Centro Vasco de Transfusión y Tejidos Humanos
- Emergencias

Cuarto - Funciones del Responsable de Seguridad de cada Organización de Servicios

Los Responsables de Seguridad de las organizaciones de servicios actuarán bajo la coordinación funcional del Responsable de Seguridad de Osakidetza-Servicio vasco de salud.

Sus funciones, siempre dentro del ámbito de su organización de servicios, son:

- Aplicar, divulgar, verificar y realizar el seguimiento de las directrices generales de seguridad de la información.
- Elaborar los informes periódicos de situación que se determinen.
- Facilitar el acceso a las dependencias en las cuales están ubicados los ficheros objeto de su responsabilidad, en base a la relación de autorizaciones emitida por el Responsable de Autorización de Accesos, ateniéndose al Procedimiento pertinente.
- Controlar el cumplimiento de la legislación vigente en materia de Protección de Datos de Carácter Personal.
- Elaborar la relación del personal de las unidades usuarias autorizado para acceder a las dependencias en las cuales están ubicados los ficheros objeto de su responsabilidad.

Quinto - Funciones del Responsable de Autorización de Accesos

En el ámbito de sus atribuciones y áreas de actuación:

- Conceder o denegar a los usuarios la autorización de acceso a los Sistemas de Información.
- Aprobar por escrito la recuperación de datos desde copias de respaldo que requiera la utilización de procesos específicos no planificados, previa autorización del Responsable de Fichero.
- Autorizar la salida de soportes informáticos que contengan Datos de Carácter Personal, previa autorización del Responsable de Fichero.
- Solicitar la actualización del Documento de Seguridad cuando la modificación de un Sistema de Información u otras circunstancias lo requieran.
- En colaboración con el Responsable de Seguridad, adoptar las medidas oportunas para que el personal usuario de Osakidetza-Servicio vasco de salud conozca las normas de seguridad que afectan al desarrollo de sus funciones y las consecuencias en que pueden incurrir en caso de incumplimiento.

Sexto – Mecanismos para facilitar el desempeño

Para facilitar el desempeño de las tareas que se deriven de las funciones enumeradas en los anteriores artículos Quinto y Sexto, la organización se halla actualmente inmersa en diversos proyectos y estudios, cuyos objetivos incluyen facilitar las herramientas y los mecanismos necesarios, que serán puestos a disposición de los responsables correspondientes, a medida que se produzca el despliegue del Plan de Implantación de las medidas de protección de datos de carácter personal.

Séptimo – Notificación y Plazo de cumplimiento

La presente Instrucción deberá notificarse a todos los Gerentes de las diferentes organizaciones de servicios de Osakidetza-Servicio vasco de salud, a fin de que adopten las medidas necesarias para su cumplimiento.

Los Gerentes de las organizaciones mencionadas en el párrafo anterior comunicarán a la Comisión de Seguridad, a través del formulario que se incluye en el **Anexo I** dirigido a su Secretario, los nombramientos a que se refiere el Artículo Segundo de la presente Instrucción, en el plazo de quince días naturales a contar desde la fecha de notificación de la misma.

Se incluye como **Anexo II**, el **procedimiento de comunicación** con la Comisión de Seguridad

En Vitoria-Gasteiz, a 30 de mayo de 2003

Fdo.: Josu I. Garay Ibáñez de Elejalde

DIRECTOR GENERAL DE OSAKIDETZA-SERVICIO VASCO DE SALUD

ANEXO I

COMUNICACIÓN DE NOMBRAMIENTOS

Organización de Servicios	X----------X

En cumplimiento de la Instrucción xxx/2003 de Dirección General, de fecha dd de mes, se disponen los siguientes nombramientos:

RESPONSABLE DE SEGURIDAD		
Servicio	**Cargo**	**Nombre y Apellidos**
X----------X	X----------X	X----------X

RESPONSABLE(S) DE AUTORIZACION DE ACCESOS		
Servicio	**Cargo**	**Nombre y Apellidos**
X----------X	X----------X	X----------X
X----------X	X----------X	X----------X
X----------X	X----------X	X----------X

En _____, a __ de _____ de 2003.

D./Dª _____

GERENTE DE _____

Inclúyase en el Documento de Seguridad.(Diríjase, mediante correo electrónico a la siguiente dirección xxxxxxxxxx)

OSAKIDETZA – S.V.S.

COMISION DE SEGURIDAD

ANEXO II

PROCEDIMIENTO

25 Marzo 2003 Versión 1.0	Procedimiento de Comunicación de la Comisión de Seguridad

OSAKIDETZA

1.1 Glosario

Se describen los términos relevantes y acrónimos utilizados en el documento.

C.S.	Comisión de Seguridad
DCP	Datos de Carácter Personal
PCA	Procedimiento de Comunicación Ascendente
PCD	Procedimiento de Comunicación Descendente
RAA	Responsable de Autorización de Accesos
RF	Responsable de Fichero
RS	Responsable de Seguridad
RSOS	Responsable de Seguridad Org. Servicio
SS.CC	Servicios Centrales

1.2 Propósito del procedimiento

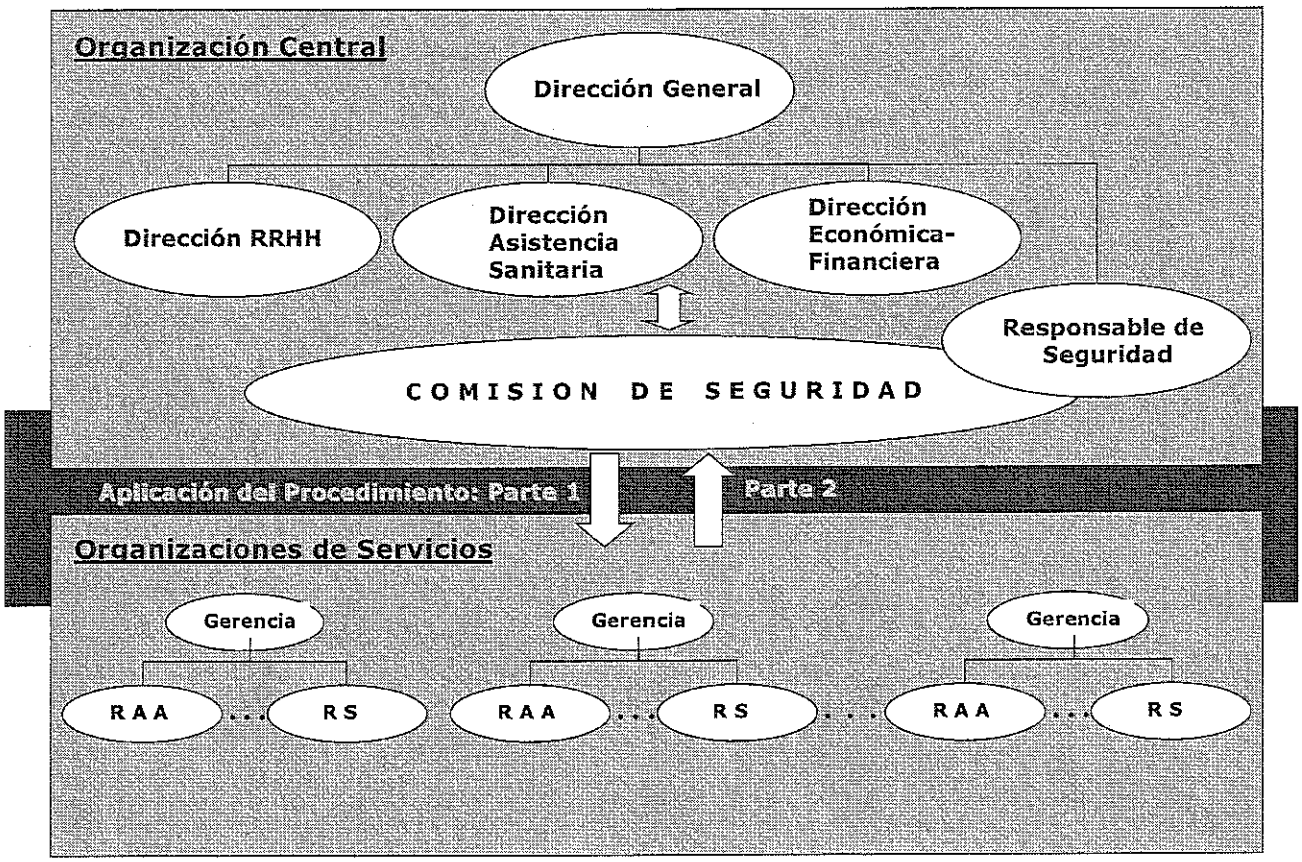
El objeto de este procedimiento es describir cómo circula, se gestiona y coordina la comunicación con la Comisión de Seguridad a lo largo del marco organizativo de Osakidetza - S.V.S en cuanto tenga relación con la protección de los Datos de Carácter Personal.

1.3 Ámbito de aplicación

El presente procedimiento debe ser conocido y respetado por las unidades siguientes:

- Servicios Centrales (SS.CC)
  - Dirección General
  - Direcciones Responsables de Fichero
    - Dirección de RR.HH
    - Dirección de Asistencia Sanitaria
    - Dirección Económico Financiera
  - Responsable de Seguridad de Servicios Centrales
  - Comisión de Seguridad (CS)
- Organizaciones de Servicios
  - Gerencias

- Responsables de Autorización de Accesos (RAA)
- Responsables de Seguridad Distribuidos (RSOS)



Marco organizativo del Procedimiento de Comunicación de la C.S.

La definición, implantación y control de la ejecución de lo establecido en este procedimiento es competencia del Responsable de Seguridad apoyado por la Comisión de Seguridad.

El proceso de comunicación quedaría organizado en dos aplicaciones:

- Por una parte, se encuentra la comunicación vertical descendente entre los organismos de los Servicios Centrales (Direcciones RF, Comisión de Seguridad y RS de SS.CC) y las Organizaciones de Servicios (Gerencias, RAA y RSOS).
- Por otra, se define el esquema comunicativo vertical ascendente entre las Organizaciones de Servicios, los Organismos de SS.CC y la Dirección General con sus Direcciones Responsables de Fichero.

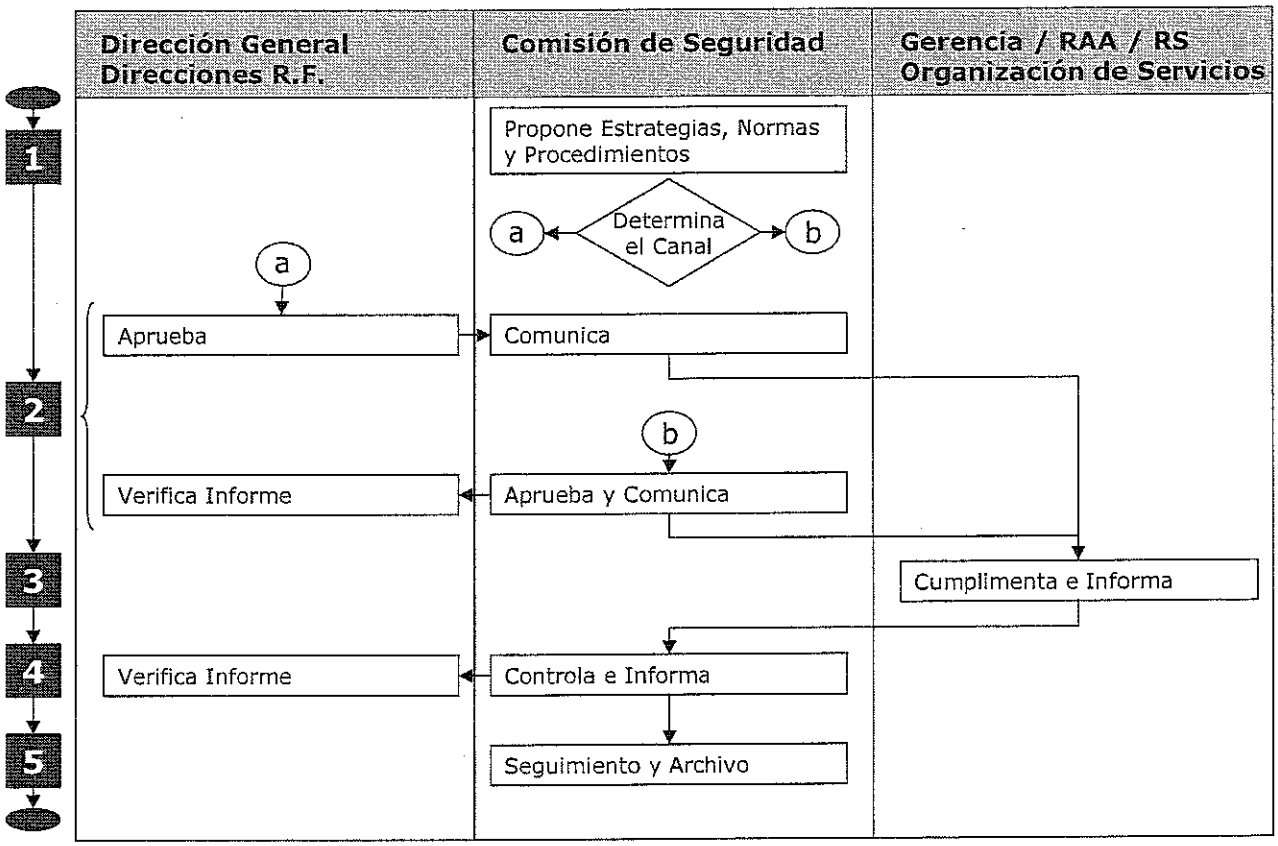
2 Comunicación vertical descendente

En los párrafos siguientes se recoge la descripción del procedimiento de comunicación vertical descendente entre la Dirección General con sus Direcciones Responsables de Fichero, Comisión de Seguridad y Responsables de las distintas Organizaciones de Servicios (Gerencias, RAA, RSOS).

2.1 Actividades del procedimiento

Código	Unidad
PCD.1.1	Proponer Estrategia, Normas o Procedimientos
PCD.1.2	Determinar el canal (A y B)
PCD.2.1	Aprobar la propuesta (según canal A) y comunicar
PCD.2.2	Aprobar la propuesta (según canal B) y comunicar
PCD.3	Cumplimentar e informar
PCD.4	Control y verificar informe
PCD.5	Seguimiento y archivo

2.2 Diagrama General del procedimiento.



Procedimiento de Comunicación de la C.S. – Descendente (Parte 1)

2.3 Descripción del procedimiento.

PCD.1.1 Proponer Estrategias, Normas y Procedimientos

La Comisión de Seguridad, en el ejercicio de las funciones que tiene atribuidas, establecerá las estrategias, normas y procedimientos pertinentes para adecuar la protección de los DCP a la normativa vigente.

PCD.1.2 Determinar el Canal: A o B

Asimismo, la Comisión de Seguridad determinará el canal oportuno (A o B) para aprobar y transmitir dicha propuesta, según su importancia relativa y la necesidad de implicación de las Direcciones Responsables de Fichero y la Dirección General en la aprobación y comunicación de la misma.

Canal A

La Comisión de Seguridad elevará a las Direcciones Responsables de Ficheros todas aquellas resoluciones relevantes en materia de seguridad para que sean aprobadas antes de proceder a su difusión y cumplimiento en las distintas organizaciones de servicios.

Canal B

La Comisión de Seguridad adoptará internamente las decisiones que no requieran la intervención de las Direcciones Responsables de Ficheros.

En este caso, se trasladará informe escrito a dichas Direcciones sobre las resoluciones acordadas.

PCD.2.1 Aprobar la propuesta (según canal A) y comunicar

En el caso de que la Comisión de Seguridad considere oportuno que la propuesta se gestione a través del canal A, será competencia de la Dirección General aprobarla y autorizar su difusión a través de la Comisión.

La Comisión de Seguridad se responsabilizará de comunicar la resolución a las organizaciones de servicios.

PCD.2.2 Aprobar la propuesta (según canal B) y comunicar

En el caso de que la Comisión de Seguridad haya decidido gestionar la "propuesta de Estrategia, Norma o Procedimiento" a través del canal B, será la propia Comisión de Seguridad la encargada de su aprobación y posterior comunicación a las diferentes organizaciones de servicios.

La Comisión de Seguridad informará por escrito sobre las resoluciones adoptadas a la Dirección General y a las Direcciones Responsables de Fichero.

PCD.3 Cumplimentar e Informar

Una vez que la resolución está aprobada y verificada se procede a su envío a cada responsable implicado en las Organizaciones de Servicios.

Dichos Responsables adoptarán las medidas oportunas para el cumplimiento de la resolución e informarán a la Comisión sobre los resultados obtenidos

PCD.4 Control y Verificación

La Comisión de Seguridad asumirá la tarea de controlar el cumplimiento de la nueva Estrategia, Norma o Procedimiento y de informar de su implantación a las Direcciones de SS.CC

Dichas Direcciones verificarán los informes aportados por la Comisión de Seguridad.

PCD.5 Seguimiento y archivo

La Comisión de Seguridad realizará las funciones de seguimiento del proceso de comunicación de resoluciones e instrucciones, así como el archivo y custodia de la documentación generada durante el mismo.

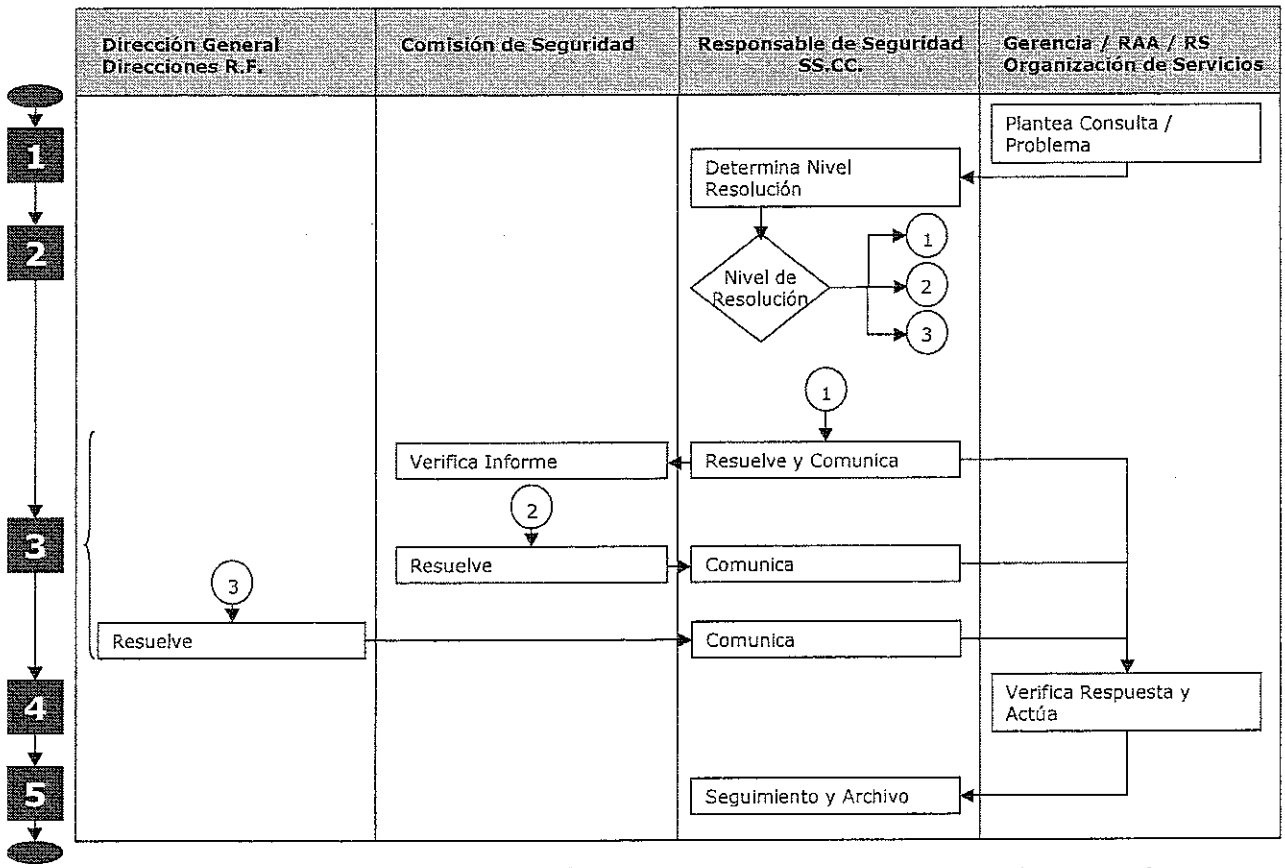
3 Comunicación vertical ascendente

En los párrafos siguientes se recoge la descripción del procedimiento de comunicación vertical ascendente entre Organizaciones de Servicios (Gerencias, RAA, RSOS), la Comisión de Seguridad, el Responsable de Seguridad de los Servicios Centrales y la Dirección General con sus Direcciones Responsables de Fichero.

3.1 Actividades del procedimiento

Codigo	Unidad
PCA.1	Plantear consulta o Problema
PCA.2	Determinar nivel de Resolución
PCA.3.1	Resolver consulta (Nivel 1) y comunicar
PCA.3.2	Resolver consulta (Nivel 2) y comunicar
PCA.3.3	Resolver consulta (Nivel 3) y comunicar
PCA.4	Verificar respuesta y actuar
PCA.5	Seguimiento y archivo

3.2 Diagrama General del procedimiento.



Procedimiento de Comunicación de la C.S. – Ascendente (Parte 2)

3.3 Descripción del procedimiento.

PCA.1 Plantear Consulta o Problema

Cuando a una de las Organizaciones de Servicios (Gerencias, RAA, RSOS) se le presente alguna duda de interpretación o de procedimiento en el cumplimiento de sus funciones, en relación con la protección de la información, planteará una "Consulta o Problema" al Responsable de Seguridad de los Servicios Centrales.

La canalización de estas consultas se realizará a través del Responsable de Seguridad de la Organización de Servicios (RSOS), de esta forma permanecerá informado de todos los pormenores relacionados con aquéllas.

PCA.2 Determinar Nivel de Resolución:1, 2 ó 3

El Responsable de Seguridad de los Servicios Centrales determinará el nivel de resolución oportuno que estima tener la consulta planteada, según el grado de colaboración que se

considere necesario por parte de la Comisión de Seguridad o de la Dirección General con sus Direcciones RF para solventarla y comunicarla.

Nivel 1

El Responsable de Seguridad de SS.CC resolverá la consulta o problema por sí mismo sin implicar directamente a la Comisión de la Seguridad ni a las Direcciones RF.

En este caso, éste transmitirá, por medio de un informe escrito, a la Comisión de Seguridad la respuesta ofrecida a las Organizaciones de Servicios.

Nivel 2

En este caso, el Responsable de Seguridad de SS.CC traslada la consulta a la Comisión de Seguridad para que se encargue de su correspondiente resolución.

Posteriormente, el Responsable de Seguridad se encargará de comunicar dicha resolución a las diferentes Organizaciones de Servicios para que adopten las medidas pertinentes.

Si la CS entendiera que la resolución de un asunto concreto le corresponde a un nivel decisorio superior, lo pondrá en conocimiento del RS para que actúe en consecuencia.

Nivel 3

El Responsable de Seguridad de SS.CC traspasa la competencia de solventar la consulta planteada a las Direcciones Responsables de Fichero o a la Dirección General.

Estas trasladarán al Responsable de Seguridad de SS.CC la resolución obtenida para su oportuna comunicación a las Organizaciones de Servicios.

PCA.3.1 Resolver consulta (Nivel 1) y comunicar

En el caso de que el responsable de Seguridad de SS.CC considere que el Nivel de Resolución 1 es el más indicado, será de su competencia resolver la consulta o problema y su correspondiente comunicación a las Organizaciones de Servicios (Gerencias, RAA, RSOS).

El Responsable de Seguridad de SS.CC también deberá mantener informada a la Comisión de Seguridad, a través de informe escrito, sobre las medidas adoptadas como resolución de la consulta o problema.

PCA.3.2 Resolver consulta (Nivel 2) y comunicar

Si la consulta o problema discurre a través del Nivel 2 de Resolución, le corresponderá a la Comisión de Seguridad solventarla e informar al Responsable de Seguridad SS.CC para que lo comunique a las Organizaciones de Servicios (Gerencias, RAA, RSOS).

En caso de que la CS entendiera que no le compete la resolución de la cuestión, lo comunicará al RS para que proceda a elevarla al siguiente nivel decisorio (Dirección General con sus Direcciones RF).

PCA.3.3 Resolver consulta (Nivel 3) y comunicar

Si se determina el 3 como Nivel de Resolución adecuado a la consulta, será la Dirección General con sus Direcciones RF las responsables de su efectiva solución.

Asimismo, las Direcciones RF deberán encargarse de su comunicación al Responsable de Seguridad de SS.CC para que éste último pueda trasladarlo a las unidades correspondientes de las Organizaciones de Servicios (Gerencias, RAA, RSOS).

PCA.4 Verificar Respuesta y Actuar

Una vez que se ha comunicado la resolución de la consulta o problema a las Organizaciones de Servicios (Gerencias, RAA, RSOS) éstas deberán verificar la respuesta obtenida y proceder a su pertinente ejecución, informando al Responsable de Seguridad de SS.CC sobre el estado de la misma.

PCA.5 Seguimiento y Archivo

El Responsable de Seguridad de SS.CC llevará a cabo las funciones de seguimiento del proceso de comunicación de resolución de consultas o problemas y el archivo y custodia de la documentación originada durante el mismo.

Soportes documentales

Los soportes documentales a utilizar en este procedimiento tendrán el carácter de comunicados internos y podrán revestir la forma de Circular, Instrucción, Resolución, etc.

Osakidetza

ACUERDO de 28 de marzo de 2003,

del Consejo de Administración de Osakidetza, por el que se crea y se asignan funciones a la Comisión de Seguridad para la Protección de Datos de Osakidetza

Septiembre 2007

Beste Iragarki Ofizial Batzuk

INDUSTRIA, MERKATARITZA ETA TURISMO SAILA

OSASUN SAILA

ARABAKO FORU ALDUNDIA

Otros Anuncios Oficiales

DEPARTAMENTO DE INDUSTRIA, COMERCIO Y TURISMO

DEPARTAMENTO DE SANIDAD

DIPUTACIÓN FORAL DE ÁLAVA

Xedapen Orokorrak

OSASUN SAILA

Zk-3490

ERABAKIA, 2003ko martxoaren 28koa, Osakidetza-Euskal Osasun Zerbitzuaren Administrazioko Kontseiluarena, Osakidetza-Euskal Osasun Zerbitzuaren datuak babesteko Segurtasun Batzordea sortu eta haren zereginak ezartzekoa.

Osakidetza-Euskal Osasun Zerbitzuaren estatutuak jasotzen dituen azaroaren 11ko 255/1997 Dekretua, eta haren edukia jarduketa zehatzen bidez garatzeak duen garratzia ikusita, egokitzat jo da «Osakidetza-Euskal Osasun Zerbitzuaren datuak babesteko Segurtasun Batzordea» sortzea eta haren zereginak ezartzea. Horretaz aparte, kontuan hartzen badugu ekainaren 1eko 994/1999 Errege Dekretua, datu pertsonalak dituzten fitxategi automatizatuen segurtasun neurriak arautzen

Disposiciones Generales

DEPARTAMENTO DE SANIDAD

Nº-3490

ACUERDO de 28 de marzo de 2003, del Consejo de Administración de Osakidetza-Servicio vasco de salud, por el que se crea y se asignan funciones a la Comisión de Seguridad para la Protección de Datos de Osakidetza-Servicio vasco de salud.

A la vista del Decreto 255/1997, de 11 de noviembre, por el que se establecen los Estatutos Sociales del ente público Osakidetza-Servicio vasco de salud y considerando la importancia de desarrollar su contenido a través de actuaciones concretas se ha valorado positivamente la propuesta de creación y asignación de funciones a la que se denominará «Comisión de Seguridad para la Protección de Datos de Osakidetza-Servicio vasco de salud» Si a esto añadimos, lo contemplado en el Real

dituena, eta erakunde publikoaren fitxategietarako prestatu den Segurtasun Agirian xedatutakoa, ezinbestekoa da batzorde hori osatzea, gai horren ingurukoak bildu eta koordinatu ditzan.

Erakunde zentralaren administrazio eta kudeaketa korporatiboaren zuzendari nagusiaren proposamena da batzordea osatzea, sortuko den batzordeari zein zeregin ezarriko zaizkien kontuan hartua, baita 12.3 artikuluak agindutakoa ere; aipatu artikuluak dioenaren arabera, erankunde zentralari baitagokio «aholkularitza eta laguntza teknikoko zerbitzu amankomunak eskaintzea, besteak beste, zerbitzu sanitarioetako erakunde bakoitzaren programa eta aurrekontuak prestatzearekin, antolakuntza eta giza baliabideekin, hirugarrenekiko kanpo harrremanekin, informazio eta komunikazio sistemekin, aholkularitza juridikoarekin, finantza kudeaketarekin, baliabide material eta zerbitzu osagarriekin, zerbitzuen jarraipen, kontrol eta ikuskapenarekin, interes orokorreko helburuen estatistikarekin, eta argitalpenekin zerikusia dutenak».

Proposamena aztertuta, jarduketa zehatz hau aipatu estatutuen 4.1 artikuluak jasotzen duen ente publikoaren ahalmenen barruan sartzen da, izan ere, artikulu horrek dioenaren arabera, Osakidetza-Euskal Osasun Zerbitzuak «nortasun juridiko publiko bereizia du, baita haren helburuak betetzeko eginbeharrekoak gauzatzeko ahalmen osoa ere»; horretaz aparte, batzordearekin lortu nahi da 3.b) artikuluan aurreikusten dena betetzea, hau da, «informazio maila eten gabe hobetzea» bereziki sustatzeko zeregina duten jarduketak burutzea.

Beraz, aurreko guztiarekin bat eginda, Administrazioko Kontseiluak adierazitakoa betetzeko eta aipatu estatutuetako 8.5 artikuluan aitortzen zaizkion eskumenen arabera, honakoa

ERABAKI DU:

Lehenengoa.– Osakidetza-Euskal Osasun Zerbitzuaren datuak babesteko Segurtasun Batzordea sortzea eta ondoren adieraziko diren eskurantzak aitortzea:

a) Zuzendaritza Nagusiari eta Erakunde Zentralaren Zuzendaritzen Zuzendaritzei segurtasun informatiko eta osasun datuen babesaren inguruko aholkularitza ematea.

b) Zerbitzuen erakunde guztien kontsultoretza, bai arreta espezializatukoetan bai lehen-mailakoetan, segurtasun informatiko eta osasun datuen babesaren inguruan, eta gai horren inguruko jarduketak koordinatzea.

c) Segurtasun informatiko eta osasun datuen babesaren inguruan baita gai horiekin zerikusia duten bestelako aspektuen inguruan ere etorkizuneko ildo estrategikoak ezartzean parte hartzea.

Decreto 994/1999, de 1 de junio, por el que se regulan las medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, y lo dispuesto en el Documento de Seguridad elaborado para los ficheros del ente público, resulta imprescindible habilitar dicha Comisión, como instrumento aglutinador y coordinador en dicha materia.

La propuesta nace de la Organización central de administración y gestión corporativa, a través de su Director General, en consideración de las funciones que se le van a asignar a la Comisión que ahora se crea y en cumplimiento del mandato del artículo 12.3, a cuyo tenor corresponde a dicha Organización central «suministrar servicios comunes de asesoramiento y apoyo técnico en relación con las funciones de programación y presupuestación de cada organización de servicios sanitarios, organización y recursos humanos, relaciones externas con terceros, sistemas de información y comunicación, asistencia jurídica, gestión financiera, gestión de medios materiales y servicios auxiliares, seguimiento, control e inspección de servicios, estadística para fines de interés general y publicaciones».

Examinada la propuesta, esta actuación concreta ha de subsumirse en la capacidad del ente público contemplada en el artículo 4.1 de los referidos Estatutos Sociales, ya que, a tenor del mismo, se reconoce para Osakidetza-Servicio vasco de salud «personalidad jurídica publica diferenciada y plena capacidad de obrar para el cumplimiento de sus fines»; y se considera que, con ella, se pretende dar debido cumplimiento a aquellas actuaciones que se refieren a la función de promover «especialmente la mejora continua de los niveles de información» prevista en el artículo 3.b).

Y, por tanto, de conformidad con la exposición que antecede, este Consejo de Administración, para debido cumplimiento de lo expuesto y en virtud de las competencias atribuidas al mismo en el artículo 8.5 de los referidos Estatutos Sociales, viene a adoptar el siguiente

ACUERDO:

Primero.– Crear la Comisión de Seguridad para la Protección de Datos de Osakidetza-Servicio vasco de salud con las atribuciones que a continuación se hacen constar:

a) Asesoramiento a la Dirección General y Direcciones de División de la Organización Central en materia de seguridad informática y protección de datos sanitarios.

b) Consultoría de todas las organizaciones de servicios, tanto de atención especializada como de atención primaria, en materia de seguridad informática y protección de datos sanitarios, coordinando las acciones en dicha materia.

c) Participación en el establecimiento de las líneas estratégicas futuras en materia de seguridad informática y protección de datos sanitarios y otros aspectos relacionados con dichas materias.

d) Prestatzen diren Segurtasun Agiriak onartzea, aldian-aldian segurtasun gaiaren inguruan egiten diren kontu-ikuskaritza txostenak gainbegiratzea, baita Segurtasun Agirian xedatutakoa behar bezala betetzen dela egiaztatzekoak ere.

e) Informazio Sistemetan eragin larria duten gertakizunen inguruko txosten esplikatzaileen analisia, baita definitzen diren bestelako Segurtasun Planen jarraipena ere.

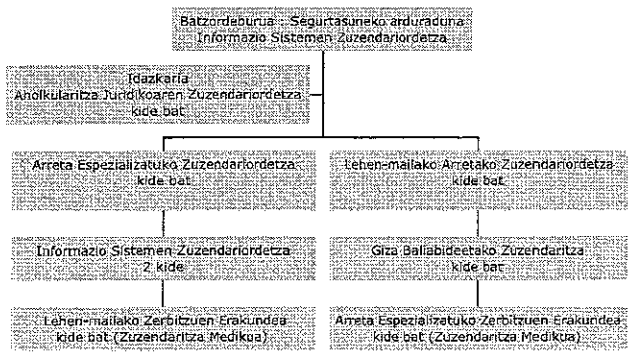
Bigarrena.– Batzordeak erakunde publikoaren kide anitzeko organo gisa funtzionatuko du, batzordea osatzeko biltzen den lehenego aldian ezartzen denari, eta Herri Administrazioen Araubide Juridikoaren eta Administrazio Prozedura Erkidearen azaroaren 26ko 30/1992 Legearen II. tituluaren II eta III kapituluek diotenari jarraiki.

Jerarkia eta zereginei dagokienez, Osakidetza-Euskal Osasun Zerbitzuaren Zuzendaritza nagusiaren menpe egongo da batzordea. Espreski, haren zereginak arinagoak izan daitezen, egoki ikusten diren lantaldeak osatu ahalko dira haren barruan, eta lantalde horien ondorioek batzordearen onespena beharko dute.

Hirugarrena.– Batzordearen zereginak gai horren inguruan indarrean dauden legeek diotenaren araberakoak izango dira, eta erabaki hau ematen den momentutik, Asistentzia Sanitarioko Zuzendaritzaren menpe dagoen Agiri klinikoak balioetsi, hautatu eta garbitzeko batzordearekin koordinazioan.

Osakidetza-Euskal Osasun Zerbitzuaren zuzendari nagusiak izendatuko ditu sortu berri den batzordeko kideak zein haien ordezkoak. Batzordeburu eta idazkaria batzordekideen artean aukeratuko ditu zuzendari nagusiak.

Laugarrena.– Batzordearen organigrama honakoa izango da, Segurtasun Agiriak dioenaren arabera



Erabaki hau indarrean sartuko da onartzen den egunean; dena den, Euskal Herriko Agintaritzaren Aldizkarian argitaratuko da eta batzordekideei banan-banako jakinarazpena egingo zaie.

Vitoria–Gasteiz, 2003ko martxoaren 28a.

Administrazioko Kontseiluburua,
GABRIEL M.ª INCLÁN IRIBAR.

d) Aprobación de los Documentos de Seguridad que se elaboren, revisión de los informes de auditoría que en materia de seguridad se emitan periódicamente y revisión de los informes de verificación del correcto cumplimiento de lo dispuesto en el Documento de Seguridad.

e) Análisis de los informes explicativos de aquellas incidencias que afecten de manera grave a los Sistemas de Información, así como el seguimiento de los diferentes Planes de Seguridad que se definan.

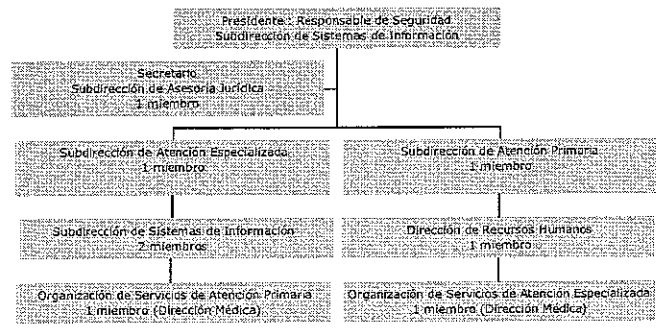
Segundo.– La referida Comisión funcionará como órgano colegiado del ente público, de conformidad con lo que se establezca en la primera sesión para constitución de la misma y en cumplimiento de los capítulos II y III del Título II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

La dependencia jerárquica y funcional será de la Dirección General de Osakidetza-Servicio vasco de salud. En particular, para agilizar el desarrollo de sus funciones, podrán crearse en su seno los grupos de trabajo que se consideren oportunos, sometiéndose sus resultados a la aprobación de la Comisión.

Tercero.– Las funciones que realice la Comisión deberán llevarse a cabo en el marco legal vigente sobre la materia y, al tiempo de dictarse este acuerdo, en coordinación con la Comisión de Documentación Clínica adscrita a la División de Asistencia Sanitaria.

Los miembros de la comisión creada o sus sustitutos serán designados por el Director General de Osakidetza-Servicio vasco de salud. El presidente y secretario serán dos miembros de esta comisión y serán también nombrados por el Director General.

Cuarto.– El organigrama de la comisión, siguiendo las pautas del Documento de Seguridad, será el siguiente:



El presente acuerdo surtirá efectos a partir de la fecha de su adopción, sin perjuicio de su publicación en el Boletín Oficial del País Vasco y notificación personal a los miembros designados para la Comisión.

En Vitoria–Gasteiz, a 28 de marzo de 2003.

El Presidente del Consejo de Administración,
GABRIEL M.ª INCLÁN IRIBAR.

Osakidetza

Instrucción Nº 6/2003 – Dirección General.

Asunto:

Funciones y obligaciones del personal de Osakidetza, con relación a la protección de datos de carácter personal. Procedimiento de actuación

Septiembre 2007

INSTRUCCIÓN 6 / 2003

DE: DIRECTOR GENERAL DE OSAKIDETZA/SERVICIO VASCO DE SALUD

A: DIRECTORES/AS GERENTES/AS ORGANIZACIONES DE SERVICIOS

ASUNTO: **Funciones y obligaciones del personal de Osakidetza/Servicio vasco de salud, con relación a la protección de datos de carácter personal. Procedimientos de actuación.**

Osakidetza/Servicio vasco de salud como parte fundamental del Sistema Sanitario de Euskadi, tiene como misión *"proveer los servicios sanitarios públicos de calidad a los ciudadanos de la Comunidad Autónoma, para satisfacer las necesidades de salud de la población, bajo los principios de equidad, eficiencia y calidad, mediante el desarrollo de actividades de promoción, prevención, cuidado y mejora de la salud"*. El personal que trabaja en las Organizaciones de Servicios de Osakidetza/ Servicio vasco de salud, como fruto de sus relaciones laborales, tiene acceso de forma total o parcial a diferentes tipos de datos: datos identificativos, datos profesionales y datos clínicos.

El contenido de esta Instrucción está dirigido a todo el personal que desarrolla su trabajo en cualquiera de las organizaciones de servicios de Osakidetza/ Servicio vasco de salud, y que en el ejercicio de sus funciones maneja sistemas de información de cualquier índole con datos de carácter personal, como: 3S-Osabide, e-Osabide, Aldabide, Gizabide, o cualquier otra aplicación informática o base de datos. La finalidad es instar a todo el personal a conocer la

normativa actual en materia de protección de los datos de carácter personal disponibles en Osakidetza/ Servicio vasco de salud, y a manejar éstos de forma confidencial y adecuada, garantizando el ejercicio de los derechos del ciudadano en esta materia.

La Ley Orgánica 15/1999, de 13 de diciembre, relativa a la Protección de Datos de Carácter Personal, es de aplicación a los datos de carácter personal registrados en cualquier soporte físico (papel, magnético o telemático) que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de los mismos. Define los ***"datos de carácter personal"*** como cualquier información concerniente a personas físicas identificadas o identificables y el ***"tratamiento de datos"*** como las 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.

Los ***"datos personales relativos a la salud"*** están especialmente protegidos, y respecto a ellos, la Ley orgánica 15/1999, en su artículo 8, dice *"las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de 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 y autonómica sobre Sanidad".*

Dada la importancia de la definición adecuada de los términos relacionados con esta normativa, se utilizara la siguiente:

- ***Contraseña***, información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.
- ***Documentación clínica***, soporte de cualquier tipo o clase que contiene un conjunto de datos e informaciones de carácter asistencial.
- ***Fichero***, todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

- ***Incidencia***, todo suceso que pueda provocar vulneración de la confidencialidad, privacidad o seguridad de los datos de carácter personal, con independencia de cual sea su soporte de registro.
- ***Información clínica***, todo dato cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla.
- ***Responsable de autorización de accesos***, persona o personas responsables de establecer los mecanismos que permiten acceder a datos o recursos.
- ***Responsable de fichero***, persona física o jurídica que decide sobre la finalidad, contenido y uso de los datos de carácter personal de un fichero.
- ***Responsable de seguridad***, persona o personas a las que el responsable de ficheros ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.
- ***Sistema de información***, conjunto de ficheros automatizados, programas soportes y equipos empleados para el almacenamiento y tratamiento de carácter personal.
- ***Soporte***, objeto físico susceptible de ser tratado en un sistema de información y sobre el que se pueden grabar o recuperar datos.
- ***Usuario***, sujeto o proceso autorizado para acceder a datos o recursos.

Así, con el fin de hacer efectivos los derechos del ciudadano, en cuanto a protección de datos y confidencialidad de la información, establecidos en la normativa actual, tal como la Ley 15/1999 de protección de datos de carácter personal, el Real Decreto 994/1999 sobre medidas de seguridad de ficheros automatizados, la Ley 41/2002 básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, la Ley 8/1997 de Ordenación Sanitaria de Euskadi, la Ley 6/1989 de Función Pública Vasca, el Decreto 272/1986 que regula el uso de la historia clínica en la Comunidad Autónoma del País Vasco (artículos 7 a 10), el Decreto 45/1998 sobre la Valoración, Conservación y Expurgo de la Documentación del Registro de Actividades Clínicas y el Decreto 175/1989 por el que se aprueba la carta de derechos y obligaciones de los pacientes y usuarios de Osakidetza/ Servicio vasco de salud, se dictan las siguientes

INSTRUCCIONES

1º.- DEBERES Y OBLIGACIONES

1.1- DEBER DE CONFIDENCIALIDAD

Todo el personal de Osakidetza/ Servicio vasco de salud que ejerce su labor en cualquiera de sus organizaciones de servicios, y que de manera directa o indirecta tenga acceso a datos de carácter personal, y/o a datos relativos a la salud (información clínica) tiene el deber de preservar la confidencialidad de los mismos, utilizarlos de forma adecuada, adoptar las medidas pertinentes para salvaguardar su confidencialidad y evitar su acceso a personal no autorizado.

El deber de secreto es independiente del tipo documental en que este recogida la información (soporte papel, magnético o telemático) y subsiste por tiempo indefinido, aún después de la finalización del contrato laboral.

Cuando por procesos de expurgo de archivo y documentación un soporte vaya a ser desechado o reutilizado, se aplicarán medidas adecuadas para salvaguardar la confidencialidad de los datos contenidos.

En el caso de empresas subcontratadas por Osakidetza/ Servicio vasco de salud y cuyo personal en el ejercicio de sus funciones, tenga acceso a datos de carácter personal, el contrato deberá incluir una cláusula específica respecto "al deber de secreto y al uso o manejo de la información estableciendo las medidas de seguridad adecuadas". En el **anexo I** figura **modelo de "cláusula sobre el deber de secreto y la confidencialidad para contratos con terceros"**.

El incumplimiento de estas obligaciones, en materia de confidencialidad y salvaguarda de la privacidad de la información, por parte del personal de Osakidetza/ Servicio vasco de salud dará lugar a la sanción que corresponda en función de la gravedad del caso (intencionalidad, perturbación del servicio, reiteración, reincidencia...), pudiendo llegar a ser causa de inhabilitación.

Si fuere detectada una violación del deber de secreto respecto a datos de carácter personal, la Dirección Gerencia de la organización de servicios correspondiente procederá a su investigación y correspondiente sanción si hubiere lugar.

1.2- DEBER DE INFORMACIÓN EN LA RECOGIDA DE DATOS

Los datos de carácter personal, incluidos los datos clínicos, sólo se podrán recoger y/o utilizar cuando sean legítimos, adecuados y pertinentes, en relación con el ámbito, finalidad y motivo para el que hayan sido obtenidos. No podrán utilizarse para finalidades incompatibles con aquellas para las que los datos fueron recogidos, o cuyo uso no está contemplado por la normativa vigente.

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

- De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

En el **anexo II**, se adjunta nota informativa de la Dirección de Asistencia Sanitaria informando a los ciudadanos del tratamiento de datos de carácter personal con la finalidad de elaborar la historia clínica informatizada, que debe estar en un lugar bien visible en las áreas de atención al cliente de las organizaciones de servicios de Osakidetza/ Servicio vasco de salud, y puede servir de **modelo para la información relativa a otros ficheros.**

1.3- OBLIGACIÓN DE RECABAR EL CONSENTIMIENTO DEL AFECTADO PARA EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

Para el tratamiento de datos de carácter personal que no estén especialmente protegidos se exige el consentimiento inequívoco del afectado, salvo las excepciones dispuestas en la legislación.

Los datos personales relativos a la salud están especialmente protegidos y cuentan con un régimen específico para su tratamiento, en atención a su destino. Así conforme al apartado 6 del art. 7 de la LOPD, y por lo que aquí interesa, los datos de carácter personal relativos a la salud podrán ser objeto de tratamiento sin consentimiento del afectado *"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 podrá ser objeto de tratamiento los datos carácter personal relativos a la salud *"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.

1.4- DEBER DE ADOPTAR MEDIDAS DE SEGURIDAD

El **responsable del fichero** deberá adoptar las medidas de índole técnica y organizativa que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

En relación a los **ficheros de carácter corporativo** las medidas se adoptarán por su correspondiente responsable desde la Organización Central de Osakidetza/ Servicio vasco de salud, sin embargo para los **ficheros de carácter no corporativos** existentes en cada organización de servicios, deberá de ser el director gerente, por medio de él o los responsables de seguridad y de autorizaciones de accesos, el encargado de articular dichas medidas, así como velar por el cumplimiento de las medidas de seguridad establecidas para cada tipo de fichero (corporativos y propios).

1.5- 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 y al deber de guarda respecto de los mismos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero, en su caso con el responsable del mismo.

1.6- OBLIGACIÓN DE RECABAR EL CONSENTIMIENTO DEL INTERESADO PARA LA CESIÓN DE DATOS DE CARÁCTER PERSONAL

La comunicación de datos de carácter personal a terceros sólo podrá realizarse para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, y con el previo consentimiento del interesado.

Si los datos pertenecen a un **fichero de carácter no corporativo**, cuando el responsable del fichero tenga necesidad de comunicar los datos de carácter personal objeto de tratamiento a un tercero, remitirá, por un medio que deje constancia del envío y de la fecha de recepción, notificación al interesado exponiendo los siguientes extremos:

- Identificación del responsable del fichero cedente.
- Datos de carácter personal del interesado en poder del responsable del fichero cuya comunicación a un tercero se pretende autorizar.
- Circunstancias en que se obtuvieron los datos que se pretende comunicar.
- Finalidad a la que se destinarán los datos cuya comunicación se pretende autorizar.
- Sujeción del cesionario, a las disposiciones de la Ley Orgánica de Protección de Datos de Carácter Personal.
- Advertencia, gráficamente destacada, de que si no se manifiesta lo contrario en el término de 15 días naturales contados a partir del día siguiente al de la recepción de la notificación, se entenderá que presta su consentimiento a la comunicación de los datos personales expuesta.
- Igualmente destacado, el carácter revocable del consentimiento prestado.

Si los datos pertenecen a un **fichero de carácter corporativo**, los responsables de dichos ficheros en la Organización Central de Osakidetza/ Servicio vasco de salud serán los competentes para decidir sobre la posible cesión.

No se requerirá el consentimiento del interesado cuando la comunicación tenga por objeto datos de carácter personal relativos a la salud y sea necesaria para solucionar una urgencia o para realizar estudios epidemiológicos en los términos establecidos en la legislación sanitaria estatal o autonómica, debiendo utilizarse para esta finalidad datos disociados.

2º.- DERECHOS Y GARANTÍAS DE LOS AFECTADOS

La solicitud de acceso, rectificación, oposición y cancelación de datos de carácter personal son derechos del ciudadano recogidos en la ley 15/1999, de protección de datos de carácter personal.

Los interesados podrán solicitar **información acerca de sus datos** y la **rectificación de los datos erróneos o innecesarios** para el fin por el que hubieren sido recogidos. Estos derechos serán ejercidos por el afectado frente al responsable del fichero, para lo que será necesario que el afectado acredite su identidad ante el responsable del fichero. 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 sus derechos.

La solicitud se acompañará de:

- Documento que acredite la identidad del interesado, como DNI u otro documento legal. Si la solicitud es del tutor o representante legal, se acompañará también la documentación que acredite esta representación.
- Exposición del motivo de la petición solicitada.
- Domicilio a efectos de notificación.
- Fecha y firma del solicitante.

Las solicitudes podrán tramitarse a través de los Servicios de Atención al Paciente y Usuario o de las Áreas de Atención al Cliente de los centros, quienes informarán debidamente a los interesados de sus derechos al respecto.

Las solicitudes se recogerán, registraran y enviarán de manera urgente al Responsable de Seguridad nombrado en cada organización de servicios, siguiendo los circuitos y procedimientos definidos, y darán lugar a una respuesta por parte del **Responsable del Fichero**, con la aprobación o denegación motivadas, enviándole al interesado una "*notificación de resolución*". En caso de tratarse de **ficheros de carácter corporativo** (Gizabide, Osabide, etc..), la solicitud se enviara a los Responsables de los ficheros en la Organización Central de Osakidetza/ Servicio vasco de salud. En cualquier caso, dada la brevedad de plazos para responder (10 días en algunos casos), será fundamental coordinar dichas acciones a fin de que los plazos se cumplan.

En el **anexo III** se adjuntan los **"Modelos de solicitudes de acceso, de rectificación y de cancelación de datos de carácter personal de los ficheros de Osakidetza/ Servicio vasco de salud".**

El responsable del fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros. Si la solicitud no reúne los requisitos expuestos en el apartado anterior, el responsable del fichero deberá requerir la subsanación de los mismos. En cualquier caso, para la respuesta se emplearán medios que permitan acreditar el envío y la recepción de la respuesta.

El responsable del fichero cuidará que el personal autorizado para acceder a los datos personales conozca y pueda prestar información a los interesados sobre sus derechos de acceso, rectificación y cancelación.

2.1- DERECHO DE ACCESO

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

El responsable del fichero resolverá sobre la solicitud de acceso en el **plazo** máximo de un mes a contar desde la recepción de la solicitud. En el caso de que no disponga de datos personales de los afectados deberá igualmente comunicárselo en el mismo plazo. Si la resolución fuese estimatoria, el acceso se hará efectivo en el plazo de los 10 días siguientes a la notificación de aquélla.

El **ejercicio del derecho de acceso** ofrecido por el responsable del fichero podrá hacerse mediante el procedimiento que sea adecuado a la configuración e implantación material del mismo (visualización en pantalla, escrito, copia o fotocopia remitida por correo...).

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

2.2- DERECHOS DE RECTIFICACIÓN Y CANCELACIÓN

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

Los derechos de rectificación y cancelación se harán efectivos por el responsable del fichero **dentro de los diez días siguientes al de la recepción de la solicitud**. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá

notificar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, a su vez, la lleve a cabo en su fichero.

La **solicitud de rectificación** deberá indicar el dato que es erróneo y la corrección que debe realizarse, debiendo ir acompañada de la documentación justificativa de la rectificación solicitada.

La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado, de terceros o cuando existiese una obligación de conservación de los datos. En este sentido y con carácter general, no procederá la cancelación de datos de la Historia Clínica en virtud del deber de conservación de la misma establecido en la legislación sanitaria.

Respecto a la **solicitud de cancelación**, el interesado deberá indicar si revoca el consentimiento otorgado en los casos en que la revocación proceda, o si por el contrario se trata de un dato erróneo o inexacto, en cuyo caso deberá acompañar la documentación justificativa. Si el responsable del fichero considera que no procede atender la solicitud del afectado, se lo comunicará motivadamente dentro del plazo de los diez días siguientes al de la recepción de la misma.

La cancelación dará lugar al bloqueo de los datos conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales. Cuando acabe el plazo de prescripción de las posibles responsabilidades nacidas del tratamiento, deberá procederse al borrado físico de los datos.

3º.- MEDIDAS DE SEGURIDAD EN LAS ORGANIZACIÓNES DE SERVICIOS

En cada Organización de Servicios, el director gerente nombrara un **Responsable de Seguridad** de cuantos Sistemas de Información estén ubicados o se generen en su ámbito de actuación. Dicho responsable de seguridad deberá garantizar la custodia eficaz de la información y documentación generada, tal como establece la normativa vigente en cuanto a medidas de seguridad de los datos de carácter personal.

A su vez, el responsable de seguridad de cada Organización de Servicios, actuará en coordinación con el responsable de seguridad de la Organización Central y con la Comisión Central de Seguridad de Osakidetza/ Servicio vasco de salud, con el fin de establecer y adoptar las medidas de seguridad más adecuadas a cada centro.

Las medidas de seguridad se establecerán de forma específica para cada sistema de información aplicando el nivel de seguridad exigible según el tipo de datos de carácter personal a tratar.

Cada sistema de información tendrá un **Responsable de Autorización de Accesos**, nombrado por el Director Gerente de la organización de servicios, que será el encargado de diseñar el sistema de accesos y tener actualizado el listado de usuarios, siendo responsable también de poner medidas para evitar el acceso a personas no autorizadas.

Las Organizaciones de Servicios deberán adecuar y adaptar el Documento de Seguridad del Ente Público Osakidetza/ Servicio vasco de salud, que define las medidas de seguridad que afectan a los ficheros de carácter corporativo existentes en el conjunto del Ente Público. Los Directores Gerente de cada organización de servicios a través del Responsable de Seguridad correspondiente, elaborarán e implantarán la normativa de seguridad a través de un **Documento de seguridad de cada Organización de Servicios**, que será producto de añadir al documento de seguridad corporativo la normativa de seguridad relativa a los ficheros propios. Para ello es necesario inventariar los ficheros no corporativos de cada organización de servicios, registrarlos en el Documento de Seguridad propio, y proceder a su declaración a la Agencia de Protección de Datos. Este Documento de Seguridad de la Organización de Servicios será de obligado cumplimiento para todo el personal que acceda a los sistemas de información.

Por lo que se refiere a los ficheros corporativos, la Comisión de Seguridad de la Organización Central revisará y actualizará de forma periódica el **documento de seguridad del Ente Público Osakidetza/ Servicio vasco de salud**, constando la fecha de revisión en el mismo.

Los Directores Gerente crearán en cada organización de servicios, una estructura de seguridad, que actuando en coordinación con la Comisión de Seguridad de la Organización Central, se encargue de:

- incorporar al Documento de Seguridad de la organización de servicios las actualizaciones que se efectúen en el Documento de Seguridad de seguridad del Ente Público Osakidetza/ Servicio vasco de salud.
- revisar periódicamente el Documento de Seguridad de la organización de servicios en lo concerniente a los ficheros propios.
- chequear las medidas establecidas para todo tipo de ficheros y de elaborar el "informe de auditoria interna" con el fin de identificar áreas de deficiencias y las medidas correctoras necesarias.

4º.- MEDIDAS DE SEGURIDAD DE LOS ORDENADORES

Para garantizar el uso adecuado de los sistemas informatizados se han de cumplir las siguientes medidas, en todos los ordenadores de las organizaciones de servicios:

- Cada usuario con acceso a sistemas de Información soportados en sistemas informatizados, tendrá asignado de forma personal, confidencial e intransferible, un *código de acceso y una contraseña*, de cuyo uso se responsabilizara personalmente.

- Cualquier sospecha de difusión o uso indebido de las contraseñas, será comunicado al Responsable de Seguridad de su organización de servicios, para su modificación, generándose la correspondiente incidencia al verse afectada la seguridad de los datos. Las contraseñas se renovarán periódicamente y el archivo/soporte donde se almacenen estará protegido.

- La protección y el uso de los *ordenadores personales, y portátiles* es responsabilidad de cada persona a la que se autoriza su uso. Si se introducen o manejan ficheros con datos de carácter personal deberán someterse a las mismas medidas de seguridad que el resto de ficheros de la organización de servicios.

- Al final de cada jornada laboral, se *apagarán los ordenadores*, y sólo se podrán mantener encendidos de forma prolongada, mediante la autorización del Responsable de Seguridad de la organización de servicios correspondiente.

5º.- NOTIFICACIÓN Y GESTIÓN DE INCIDENCIAS

Incidencia es todo suceso que pueda provocar vulneración de la confidencialidad, privacidad o seguridad de los datos de carácter personal, con independencia de cual sea su soporte de registro.

Las incidencias que puedan acontecer durante la explotación de los sistemas de información de Osakidetza/ Servicio vasco de salud, y que traten datos de carácter personal, deberán quedar registrados en un **libro de incidencias** por medio del llamado **informe de incidencias**, comunicándose al Responsable de Seguridad de la organización de servicios, debiendo recoger:

- Descripción de la incidencia
- Fecha y hora en la que se produce
- Centro o dependencia donde se ha producido
- Nombre y apellidos de la persona que notifica

El **anexo IV**, contiene el modelo de "***Informe de notificación de incidencias***" que se utilizara en estos casos.

A efectos operativos y de inspección, se guardarán o mantendrá el registro de las incidencias acaecidas en los últimos 12 meses. Cuando el tipo de incidencia, de lugar a una "*recuperación de datos*", se describirá el procedimiento usado para la recuperación y grabación.

Los responsables de seguridad de cada organización de servicios, una vez detectada una incidencia y en función de la gravedad de la misma, la comunicaran al Director Gerente de la misma y al Responsable de Seguridad de la Organización Central, para depurar las posibles responsabilidades.

Las Direcciones Gerencia de las organizaciones de servicios, a través de las direcciones que de ellas dependen y de las jefaturas de unidades, servicios o áreas de atención al cliente implicados, establecerán los mecanismos necesarios para el cumplimiento de esta Instrucción y para su difusión al personal de Osakidetza/ Servicio vasco de salud implicado.

En Vitoria-Gasteiz, a 2 de septiembre de 2003

Josu I. Garay Ibáñez de Elejalde
Director General de Osakidetza/ Servicio vasco de salud

ANEXO I. CLAUSULA SOBRE EL DEBER DE SECRETO Y CONFIDENCIALIDAD PARA CONTRATOS CON TERCEROS

En consideración al tipo de información procesada en el desempeño de su labor, el personal del adjudicatario está obligado a mantener la más absoluta confidencialidad sobre todos aquellos datos y documentos a que tengan acceso con motivo de esta adjudicación. A ellos accederán, exclusivamente, las personas estrictamente imprescindibles para el desarrollo de las tareas inherentes a la misma. Todas ellas serán advertidas del carácter confidencial y reservado de la información a la que tendrán acceso.

Todos los ficheros que se pongan a disposición del adjudicatario para la ejecución del contrato son propiedad de **Osakidetza** y están registrados y sometidos a la salvaguarda que establece la legislación vigente, en especial la relativa a la protección de datos personales. Toda cesión a terceros será perseguida en los tribunales.

Los citados datos o ficheros no podrán ser empleados ni tratados por la empresa xxx para fin distinto al previsto en el contrato de xxxx, estando especialmente prohibida su cesión o comunicación a terceros. Una vez cumplida la prestación contractual principal, los datos de carácter personal deberán ser destruidos por la adjudicataria.

Osakidetza se reserva el derecho de establecer cualquier tipo de marcaje de los ficheros que se dejarán al adjudicatario, de manera que sus características puedan constituirse como prueba que posibilite localizar el origen y los responsables de las eventuales cesiones.

Bajo ningún caso ni circunstancia, el adjudicatario podrá suministrar a terceros, ni utilizar para sí ni para otros, datos facilitados por **Osakidetza**, para fines distintos a los contemplados en el objeto del presente contrato.

El adjudicatario estará obligado a poner en conocimiento de **Osakidetza**, inmediatamente después de ser detectada, cualquier sospecha de eventuales errores que se puedan producir en el sistema de seguridad de la información.

El adjudicatario faculta a **Osakidetza** para que, al terminar el proyecto, pueda responsabilizarlo y/o repercutirle los costes derivados de posibles reclamaciones ocasionadas por negligencia y/o falta de confidencialidad del mismo.

ANEXO II- MODELO DE INFORMACION AL USUARIO SOBRE RECOGIDA DE DATOS DE CARÁCTER PERSONAL PARA SU INCORPORACION A FICHERO INFORMATIZADO

Mediante la presente "Nota Informativa", la Dirección de Asistencia Sanitaria de Osakidetza-Servicio vasco de salud pone en conocimiento de los ciudadanos que los datos personales que se les soliciten, serán objeto de tratamiento e incorporados a los ficheros de datos de carácter personal que existen en Osakidetza-Servicio vasco de salud.

La recogida y tratamiento de los datos personales solicitados por los profesionales sanitarios y no sanitarios de Osakidetza-Servicio vasco de salud tiene como finalidad la elaboración de la historia clínica de los pacientes para el seguimiento de su estado de salud, la gestión adecuada de los servicios sanitarios, la investigación científica y la actividad docente.

El responsable del fichero de historia clínica es la Dirección de Asistencia Sanitaria (c/ Alava, 45 - 01006 Vitoria-Gasteiz), órgano al que Vds. deberán dirigirse para ejercer los derechos de acceso, rectificación y cancelación.

Los datos que como titular Vd. facilite únicamente serán cedidos a otros organismos del sistema sanitario y organismos oficiales de estadística. Cualquier cesión fuera de las previstas requerirá su expreso consentimiento, salvo que se trate de solucionar una urgencia o para realizar estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal y autonómica.

Es todo cuanto se comunica en cumplimiento del deber de información que impone el artículo 5 de la Ley 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.
Atentamente,

DIRECTOR ASISTENCIA SANITARIA

OSAKIDETZA-SERVICIO VASCO DE SALUD

ANEXO III. FORMULARIO DE SOLICITUD DE ACCESO A DATOS DE CARÁCTER PERSONAL DE FICHEROS DE OSAKIDETZA/SERVICIO VASCO DE SALUD.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:

Dirección de la oficina de acceso:

DATOS DEL SOLICITANTE

D/Dª ....., mayor de edad, con domicilio en la C/....., nº....., Localidad....., Provincia.....,CP....., con DNI ....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con los artículos 15 de la Ley Orgánica de Protección de Datos de Carácter Personal, LO 15/1999, y los artículos 12 y 13 del Real Decreto 1332/94.

SOLICITA:

1.- Que se le facilite gratuitamente acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, entendiendo que si transcurre este plazo sin que de forma expresa se conteste a la mencionada petición de acceso se entenderá denegada. En este caso se interpondrá la oportuna reclamación ante la Agencia de Protección de Datos para iniciar el procedimiento de tutela de derechos, en virtud del artículo 18 de la Ley Orgánica y 17 del Real Decreto.

2.- Que si la solicitud del derecho de acceso fuese estimada, se remita por correo la información a la dirección arriba indicada en el plazo de diez días desde la resolución estimatoria de la solicitud de acceso.

3.- Que esta información comprenda de modo legible e inteligible los datos de base que sobre mi persona están incluidos en sus ficheros, y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En ....., a.....de .....de 200

ANEXO III. FORMULARIO DE SOLICITUD DE RECTIFICACION DE DATOS DE CARÁCTER PERSONAL DE FICHEROS DE OSAKIDETZA/SERVICIO VASCO DE SALUD.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:

Dirección de la oficina de acceso:

DATOS DEL SOLICITANTE

D/Dª ....., mayor de edad, con domicilio en la C/....., nº....., Localidad....., Provincia.....,CP....., con DNI ....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de rectificación, de conformidad con los artículos 16 de la Ley Orgánica de Protección de Datos de Carácter Personal, LO 15/1999, y los artículos 15 y 16 del Real Decreto 1332/94.

SOLICITA:

1.- Que se proceda gratuitamente a la efectiva corrección en el plazo de diez días desde la recepción de la solicitud, de los datos inexactos relativos a mi persona que se encuentran en sus ficheros.

2.- Los datos que hay que rectificar se enumeran en la hoja anexa, haciendo referencia a los documentos que se acompañan a esta solicitud y que acreditan, en caso de ser necesario, la veracidad de los nuevos datos.

3.- Que me comuniquen de forma escrita a la dirección arriba indicada, la rectificación de los datos una vez realizada.

4.- Que, en el caso de que el responsable del fichero considere que la rectificación o la cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley.

En ....., a.....de .....de 200

ANEXO III. FORMULARIO DE SOLICITUD DE CANCELACION DE DATOS DE CARÁCTER PERSONAL DE FICHEROS DE OSAKIDETZA/SERVICIO VASCO DE SALUD.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:

Dirección de la oficina de acceso:

DATOS DEL SOLICITANTE

D/Dª ....., mayor de edad, con domicilio en la C/....., nº....., Localidad....., Provincia.....,CP....., con DNI ....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de cancelación, de conformidad con los artículos 16 de la Ley Orgánica de Protección de Datos de Carácter Personal, LO 15/1999, y los artículos 15 y 16 del Real Decreto 1332/94.

SOLICITA:

1.- Que se proceda a la efectiva supresión en el plazo de diez días desde la recepción de esta solicitud, de cualesquiera datos relativos a mi persona que se encuentren en sus ficheros al no existir vinculación o disposición legal que justifique su mantenimiento.

2.- Que me comuniquen de forma escrita a la dirección arriba indicada la cancelación de datos una vez realizada.

3.- Que, en el caso de que el responsable del fichero considere que dicha cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley.

En ....., a.....de .....de 200

ANEXO IV. INFORME DE NOTIFICACIÓN DE INCIDENCIAS

INCIDENCIA Nº _____ **Fecha notificación:** _____

Nombre y Apellidos de quien notifica:_____

Cargo o puesto: _____

Tipo de incidencia:

Descripción (detallada): _____

_____

_____

_____

_____

Fecha y hora en la que se produjo: _____

Efectos que puede producir: (en caso de no subsanación o incluso independiente de ello)

Recuperación de datos: SI ☐ NO ☐ No Procede ☐

Procedimiento realizado: ____

Datos restaurados: _____

Datos grabados manualmente: _____

Persona que ejecutó el proceso: _____

- Nombre:
- Apellidos:
- D.N.I.
- Firma:

Firma de quien notifica