17

Manual de Buenas Prácticas para entidades locales de la Comunidad Autónoma del País Vasco en materia de PROTECCIÓN DE DATOS PERSONALES

EUDEL

Tirada: 1500 ejemplares

Edita: **EUDEL. Asociación de Municipios Vascos**
Internet: www.eudel.net
Impresión: GRAFILUR S.A.
D.L.: BI-1237-08

En la elaboración de este **Manual de Buenas Prácticas** han colaborado las siguientes personas:

Ana Novoa Carbarllido, Ayuntamiento de Vitoria-Gasteiz
Enrique Pascual Antxia, Ayuntamiento de Basauri
José Antonio Fernández Celada, Ayuntamiento de Ermua
Javier Aramberri Miranda, Ayuntamiento de Getxo
José Luis Irigoien Martínez, Ayuntamiento de Eibar
Julen Urteaga Legarra, Ayuntamiento de Beasain
Iñaki Galdeano Larizgoitia, EUDEL
Ignacio Alonso Errazti, EUDEL
Pedro Alberto González González, AVPD
Pablo Lakuntza Amiano, AVPD
Edurne Barañano Etxebarria, AVPD
Aintzane Osa Alberdi, traducción al euskera, AVPD
Simón Mesanza Legarda, AVPD

PRESENTACIÓN

La protección de datos es un derecho muy poco conocido. Los pocos estudios que existen al respecto evidencian un alto grado de desconocimiento en la ciudadanía de su propio derecho, así como de la existencia de autoridades de control. Dentro de los Ayuntamientos de Euskadi, el grado de sensibilidad es muy variable. Un número importante de Ayuntamientos cumple sus obligaciones formales (creación y declaración de ficheros), un grupo menor cumple el resto de obligaciones que la ley impone y son muy pocos los que tienen establecidas “conductas organizativas” donde la protección de datos sea un eje transversal que ligue toda su actuación administrativa. Por otra parte, somos conscientes de que, en muchas ocasiones, el grado de cumplimiento está directamente relacionado con el tamaño del municipio y con los recursos personales y materiales que tiene a su disposición.

Esta nueva publicación que la Asociación de Municipios Vascos, EUDEL, presenta a los Ayuntamientos es fruto de una actuación coordinada con la Agencia Vasca de Protección de Datos, AVPD. Juntos hemos impulsado la creación de un grupo de trabajo para conocer y debatir actuaciones y comportamientos de las entidades locales relacionados con la protección de datos de carácter personal, estudiar la casuística más frecuente, las “colisiones” que la aplicación de este derecho puede tener con otros y, con todo ello, proponer un Manual de Buenas Prácticas que facilite una “adaptación” de la normativa a las realidades concretas donde se tiene que aplicar.

El Manual de Buenas Prácticas tiene la naturaleza de Código Tipo de las entidades locales de Euskadi, y su objeto es adecuar lo establecido en la normativa sobre protección de datos de carácter personal a las peculiaridades de los tratamientos efectuados por las entidades locales de la CAPV fomentando una mayor concienciación en el campo de la protección de datos de carácter personal entre las entidades locales y las personas que trabajan a su servicio.

En el grupo de trabajo han participado representantes de EUDEL, la AVPD y los Ayuntamientos de Vitoria-Gasteiz, Basauri, Getxo, Ermua, Eibar y Beasain. Se han realizado muchas sesiones de trabajo y reuniones de coordinación durante más de un año, habiendo contribuido todos los miembros con importantes aportaciones. A todos ellos, nuestro más sincero agradecimiento, ya que son los verdaderos protagonistas de la existencia del Manual y de las oportunidades que ofrece.

Este Manual sólo supone el principio de lo que esperamos sea una fructífera relación de la AVPD, EUDEL y las entidades locales para que asuman cambios organizativos importantes relacionados con el derecho a la privacidad. Las ciudadanas y ciudadanos depositan una gran confianza en sus Ayuntamientos y demandan un especial rigor en el tratamiento de sus datos. El Manual es una herramienta que, además de una parte dispositiva, acompaña cuadernillos independientes con multitud de modelos y documentos, esquemas de procedimientos tipo y supuestos concretos que permitirán a los Ayuntamientos el asumirlos o adaptarlos.

Hasta ahora hemos sido nosotros los protagonistas, EUDEL, la AVPD y, fundamentalmente, los miembros del grupo de trabajo. Ahora ha llegado vuestro momento. El momento de que vuestros Ayuntamientos y Entidades se adhieran al Manual, lo hagan suyo y realicen las adaptaciones que sean necesarias en su forma de actuar para respetar el derecho a la protección de datos y reforzar la confianza en ellos depositada.

Jokin Bildarratz Sorron
Presidente de EUDEL

Iñaki Vicuña de Nicolás
Director de la AVPD

Índice

3. OBLIGACIONES DE LA ADMINISTRACIÓN Y SU PERSONAL 33-66

3.1. CUMPLIMIENTO DE REQUISITOS FORMALES 34

3.2. RECOGIDA Y TRATAMIENTO DE DATOS PERSONALES 36

3.3. RESPECTO DE LOS DERECHOS DE LAS PERSONAS 40

3. OBLIGACIONES DE LA ADMINISTRACIÓN Y SU PERSONAL 33-66

3.4. EN SUS RELACIONES CON TERCERAS PERSONAS O ENTIDADES 41

3.5. MEDIDAS DE SEGURIDAD DE LOS FICHEROS 45

4. CONCURRENCIA DEL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL CON OTROS DERECHOS 67-78

4.1. DERECHO A LA PROTECCIÓN DE DATOS Y DERECHO DE ACCESO A LA INFORMACIÓN 68

4.2. DERECHO A LA PROTECCIÓN DE DATOS Y PUBLICACIÓN 73

DISPOSICIONES GENERALES

Artículo 1. Objeto

1. Este Manual de Buenas Prácticas tiene por objeto **regular el tratamiento de los datos de carácter personal que realizan las entidades locales,** los organismos autónomos dependientes de ellas, así como de las sociedades dependientes o vinculadas a ellas cuando su capital sea de mayoría pública y ejerzan potestades públicas, existentes en el ámbito territorial de la Comunidad Autónoma del País Vasco (en adelante entidades locales de la CAPV o entidades locales), **a fin de garantizar y proteger las libertades públicas y los derechos fundamentales de los ciudadanos y ciudadanas** que se relacionan con ellas y, especialmente, **su derecho al honor e intimidad personal y familiar,** en el marco del respeto a lo establecido en la Ley Orgánica de Protección de Datos de Carácter Personal y su normativa de desarrollo.

2. Asimismo tiene la finalidad de convertirse en un Código Tipo o Guía Práctica que sirva para facilitar información al personal al servicio de las entidades locales de la CAPV acerca de la manera de actuar en su relación con los ciudadanos y ciudadanas, en todo lo referente al tratamiento de datos personales.

Artículo 2. Ámbito de aplicación

1. Este Manual será de aplicación a todo tratamiento de los datos de carácter personal que figuren en ficheros, automatizados o no, de las entidades locales de la CAPV y a toda modalidad de uso posterior de estos datos.

2. La adhesión a este Manual de Buenas Prácticas o Código Tipo será voluntaria para las entidades locales de la CAPV, sin perjuicio de la obligación que les incumbe de cumplir con la normativa vigente de protección de datos. Una vez que una entidad local se adhiera a este Manual de Buenas Prácticas o Código Tipo quedará obligada a su cumplimiento.

La adhesión a este Manual será voluntaria para las entidades locales de la CAPV, sin perjuicio de la obligación de cumplir con la normativa vigente de protección de datos

Artículo 3. Datos de carácter personal

1 En las entidades locales se tratan diariamente datos de carácter personal. Estos datos se refieren principalmente a los ciudadanos y ciudadanas, al personal al servicio de cada entidad local, a empresas proveedoras, etc.

2 Para el desempeño de las competencias que tienen atribuidas, las entidades locales deben crear ficheros que contienen datos de carácter personal y gestionar estos datos. Asimismo deben **cumplir la normativa de protección de datos** de carácter personal **al solicitar, recoger, tratar, utilizar o ceder datos** de las personas con las que se relacionan. Además, dado que se trata de un derecho fundamental de nueva generación, habrán de poner los medios necesarios para extender la nueva cultura de la protección de datos en sus procedimientos y entre el personal a su servicio.

Las entidades habrán de poner los medios necesarios para extender la nueva cultura de protección de datos

3 **Las entidades locales de la CAPV han de declarar los ficheros en la Agencia Vasca de Protección de Datos** (en adelante AVPD), antes de recabar datos de carácter personal con destino a los mismos, y han de prestar especial atención al consentimiento de las personas cuando los datos recabados tengan la consideración de especialmente protegidos.

Artículo 4. Legislación aplicable

1 En el **Anexo V** relativo a la legislación y normativa en materia de protección de datos personales se reproducen las principales normas de aplicación que las entidades locales de la CAPV deberán respetar:

- 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.

- Artículo 18 de la Constitución Española.

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD).

- 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.

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos. (BOPV 16 de noviembre de 2005).

- Decreto 309/2005, de 18 de octubre, por el que se aprueba el Estatuto de la Agencia Vasca de Protección de Datos. (BOPV 9 de noviembre de 2005).

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

- Resolución de 28 de noviembre de 2005, del Director de la Agencia Vasca de Protección de Datos por la que se desarrolla la estructura orgánica de la Agencia Vasca de Protección de Datos.
- Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.
- Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

2 En el supuesto de que se produzcan cambios legislativos o normativos, las referencias realizadas en este Manual de Buenas Prácticas a las disposiciones vigentes a su entrada en vigor, serán consideradas como realizadas a las que las sustituyan.

Actualización periódica del Manual de Buenas Prácticas

3 Este Manual de Buenas Prácticas será periódicamente actualizado en función de los nuevos requerimientos legales o normativos que puedan ser exigidos, de conformidad con lo establecido en la Disposición Final.

1 Conceptos básicos

- **Datos de carácter personal**

  Cualquier información (numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo) concerniente a personas físicas identificadas o identificables.

- **Persona identificable**

  Toda persona cuya identidad pueda determinarse directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas.

- **Datos especialmente protegidos**

  Datos que se refieren a ideología, religión, creencias, afiliación sindical, origen racial, salud, vida sexual o infracciones penales o administrativas.

- **Fichero**

  Todo conjunto organizado de datos de carácter personal, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso.

- **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.

- **Persona afectada o interesada**

  Persona física a la que se refieren los datos que son objeto de tratamiento.

- **Procedimiento de disociación**

  Es un tratamiento de datos personales por el que se obtiene una información que no puede asociarse a una persona identificada o identificable.

- **Responsable interno**

  Persona al servicio de la administración que, por delegación del órgano competente, realiza las tareas encargadas a la persona Responsable del Fichero.

- **Persona Encargada del tratamiento**

  La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta de la administración interesada.

- **Consentimiento de la persona interesada**

  Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual, la persona interesada consiente el tratamiento de datos personales que le conciernen.

- **Cesión o comunicación de datos**

  Toda revelación de datos realizada a una persona distinta de la interesada.

- **Persona destinataria o cesionaria**

  La persona física o jurídica, pública o privada, u órgano administrativo, al que se revelen los datos. En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará tercera a la persona o personas integrantes de los mismos.

- **Tercera**

  La persona física o jurídica, autoridad pública o privada, u órgano administrativo, distinta de la persona afectada o interesada, de la Responsable interna del Fichero, de la Encargada del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa de la persona Responsable interna del Fichero o de la Encargada del tratamiento. En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará tercera a la persona o personas integrantes de los mismos.

- **Fuentes accesibles al público**

  Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencias 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.

2 Conceptos relacionados con medidas de seguridad

- **Sistemas de información**

  Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

- **Usuario/a**

  Persona o proceso autorizado para acceder a datos o recursos.

- **Recurso**

  Cualquier parte componente de un sistema de información.

- **Accesos autorizados**

  Autorizaciones concedidas a una persona usuaria para la utilización de los diversos recursos.

- **Identificación**

  Procedimiento de reconocimiento de la identidad de una persona usuaria.

- **Autenticación**

  Procedimiento de comprobación de la identidad de una persona usuaria.

- **Control de acceso**

  Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

- **Contraseña**

  Información confidencial, frecuentemente constituida por una cadena de caracteres que puede ser usada en la autenticación de una persona usuaria.

- **Incidencia**

  Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

- **Bloqueo**

  La identificación y reserva de datos de carácter personal con el fin de impedir su tratamiento excepto por parte de las administraciones públicas, Jueces y Juezas y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades.

- **Borrado o supresión**

  La eliminación física de los datos de carácter personal bloqueados una vez cumplido el plazo de prescripción de las posibles responsabilidades nacidas del tratamiento de dichos datos.

- **Soporte**

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

- **Responsable de Seguridad**

  Persona o personas a las que la persona Responsable del Fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

- **Copia de respaldo**

  Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

2

DERECHOS DE LOS CIUDADANOS Y CIUDADANAS

Artículo 6. Derecho a la información sobre el uso y finalidad de los ficheros

1. Las personas a las que desde las **entidades locales** se soliciten datos personales deberán ser **previamente informadas** 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 o destinatarias de la información.

   b) Del carácter obligatorio o facultativo de su respuesta a las preguntas o soluciones de información 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 de la persona responsable del tratamiento.

2. El artículo 5 de la LOPD establece que no será necesaria la información de los apartados b), c) y d) anteriores si se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. No obstante, se informará siempre a las personas interesadas de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición y del órgano ante el que se podrán ejercitar tales derechos.

3. La información se proporcionará a través de un medio coherente con el sistema de recogida de los datos; por ejemplo, si se recogen mediante cuestionarios o impresos, las informaciones y advertencias anteriores deberán figurar claramente en los mismos, debiéndose procurar que el tipo y tamaño de la letra empleada sea el mismo que el de los demás contenidos del documento.

Las informaciones sobre los derechos de las personas y otras advertencias deberán figurar claramente

4 Si las consideraciones de diseño o composición del documento a emplear aconsejasen el recurso a un tipo o tamaño de letra más reducido, se complementará la información a suministrar a través de carteles instalados en un lugar visible y destacado en las oficinas de atención ciudadana, y si la entidad local afectada dispusiera de página Web, también se ofrecerá dicha información mediante su publicación en la misma.

5 **Cuando** los datos de carácter personal **no hayan sido recabados de la persona interesada,** ésta **deberá ser informada de forma expresa,** precisa e inequívoca, por la entidad local dentro de los tres meses siguientes al momento de registro de los datos, salvo que ya hubiera sido informada con anterioridad, del contenido del tratamiento, de la procedencia de los datos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, y de la identidad y dirección de persona responsable del tratamiento.

6 Con el fin de llevar el derecho de información a su máxima expresión, **la entidad local informará de la existencia de este Manual de Buenas Prácticas** cuando recoja datos personales a través de formularios, indicando su ubicación en Internet, en la Web de la propia entidad local, en su caso, y en las de EUDEL y de la AVPD, para su consulta.

7 Los **Anexos M1.1, M1.2 y M1.3 del Anexo II** incluyen los modelos de cláusula informativa para la recogida de información, para publicar y una específica para procesos selectivos.

Artículo 7. Derecho de acceso

Los ciudadanos y ciudadanas tienen derecho a solicitar y obtener de su entidad local información sobre sus datos de carácter personal

1 Los ciudadanos y ciudadanas tienen derecho a solicitar y obtener de su entidad local información de sus datos de carácter personal sometidos a tratamiento, del origen de dichos datos, así como de las comunicaciones realizadas o que se prevén hacer de los mismos.

2 **El derecho de acceso** a que se refiere este artículo sólo podrá ser ejercitado en **intervalos iguales o superiores a doce meses,** salvo que la persona interesada acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

3 Existe un modelo de formulario para el ejercicio del derecho de acceso en el **Anexo II M2.** En el mismo se incluye información sobre las normas de aplicación y las condiciones y plazos para su ejercicio, tramitación y atención.

Artículo 8. Derecho de rectificación

1 Cuando **la persona titular de los datos** tuviera constancia de que sus datos personales tratados en un fichero son inexactos, inadecuados, incompletos o excesivos, **podrá solicitar y obtener de la entidad local que los rectifique, corrija o complete.**

2 Existe un modelo de formulario para el ejercicio del derecho de rectificación en el **Anexo II M3.** En el mismo se incluye información sobre las normas de aplicación y las condiciones y plazos para su ejercicio, tramitación y atención.

Artículo 9. Derecho de cancelación

1 La persona titular de los datos podrá solicitar y obtener de la entidad local la cancelación de los mismos cuando:

- Hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recabados.
- Se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recabados.

2 No obstante, 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 entidad local y la persona interesada.

3 Existe un modelo de formulario para el ejercicio del derecho de cancelación en el **Anexo II M4.** En el mismo se incluye información sobre las normas de aplicación y las condiciones y plazos para su ejercicio, tramitación y atención.

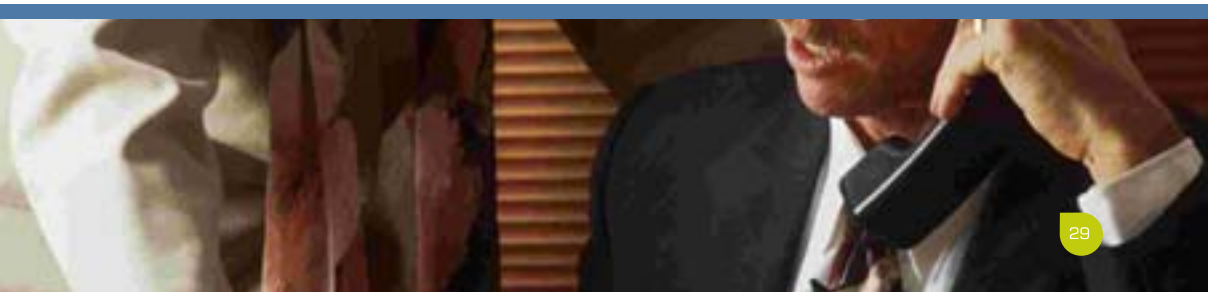
Una vez que se ha cumplido la finalidad para la que fueron recabados los datos personales es obligatorio cancelarlos, primero, en su caso, bloqueándolos y después suprimiéndolos

Artículo 10. Derecho de oposición

1 Los ciudadanos y ciudadanas tienen derecho a oponerse a un tratamiento de datos por la entidad local cuando, sin ser preceptivo el consentimiento previo, existan motivos fundados y legítimos relativos a su concreta situación personal.

2 Las personas interesadas pueden oponerse a un tratamiento de sus datos personales, en cualquier momento, incluso cuando siendo preceptivo el consentimiento previo, lo hubieran prestado con anterioridad.

3 Existe un modelo de formulario para el ejercicio del derecho de oposición en el **Anexo II M5.** En el mismo se incluye información sobre las normas de aplicación y las condiciones y plazos para su ejercicio, tramitación y atención.



Artículo 11. Ejercicio de los derechos de acceso, rectificación, cancelación y oposición

1. Cualquier petición de acceso, rectificación, cancelación u oposición sobre datos de carácter personal se realizará **mediante escrito dirigido a la persona Responsable del Fichero** de la entidad local interesada, a través del Registro General o por cualquiera de los medios previstos en la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Cuando la presentación de la petición no se haga de manera presencial la acreditación de la identidad de la persona interesada se podrá realizar por cualquier medio admitido en Derecho.

2. Los derechos de acceso, rectificación, cancelación u oposición de datos son personalísimos y serán ejercidos únicamente por la persona interesada. No obstante, ésta podrá actuar a través de la persona que designe como representante legal cuando se encuentre en situación de incapacidad legal o en minoría de edad que le imposibilite el ejercicio personal de los mismos, en cuyo caso será necesario que la persona que actúe como representante legal acredite tal condición.

Los derechos de Acceso, Rectificación, Cancelación u Oposición son gratuitos y podrán ejercerse a través de representante legal acreditado en los casos de minoría de edad o incapacidad legal

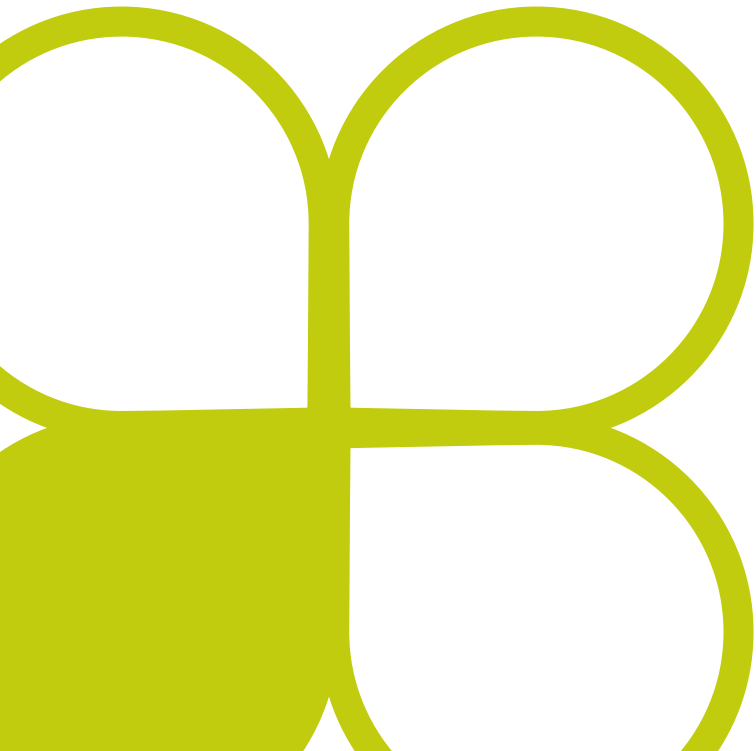
3. No se exigirá contraprestación alguna por el ejercicio de los derechos de acceso, rectificación, cancelación u oposición de datos de carácter personal.

Artículo 12. Derecho a la impugnación de valoraciones

Las personas interesadas tendrán derecho a impugnar decisiones que les afecten significativamente y que se basen en valoraciones realizadas por la entidad local basadas únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. Esta impugnación se ejercitará como derecho de oposición.

Artículo 13. Derecho a indemnización por daño o lesión en los bienes y derechos de las personas

Las personas que, como consecuencia del incumplimiento de lo dispuesto en la normativa de protección de datos por la persona responsable o la encargada del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizadas. Esta responsabilidad se exigirá de conformidad con lo dispuesto en la legislación reguladora del régimen de responsabilidad de las administraciones públicas.



Artículo 14. Solicitud de tutela ante la Agencia Vasca de Protección de Datos

1. Cualquier persona interesada a la que se deniegue, total o parcialmente, el ejercicio de los derechos de acceso, rectificación, oposición o cancelación, o entienda que no se le ha facilitado o atendido el ejercicio de su derecho, puede reclamar ante la Agencia Vasca de Protección de Datos para que inicie un procedimiento de tutela de sus derechos.

2. En la página Web de la AVPD (www.avpd.es), en el apartado ciudadanos, hay modelos para solicitar el inicio del procedimiento de tutela de los derechos.

Cualquier persona interesada a la que se deniegue el ejercicio de los derechos de acceso, rectificación, oposición u cancelación puede pedir la tutela de la Agencia Vasca de Protección de Datos

3

OBLIGACIONES DE LA ADMINISTRACIÓN Y SU PERSONAL

3.1. CUMPLIMIENTO DE REQUISITOS FORMALES

Artículo 15. Creación, modificación y supresión de ficheros

1. La creación, modificación o supresión de ficheros corresponde al órgano competente de cada entidad local. La resolución o acuerdo por el que se aprueben los ficheros será objeto de **publicación en el Boletín Oficial del Territorio Histórico.**

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

- La identificación y la finalidad del fichero y los usos previstos para el mismo.
- Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
- El procedimiento de recogida de los datos de carácter personal.
- La estructura básica del fichero.
- La descripción de los tipos de datos de carácter personal incluidos en el mismo.
- Las cesiones de datos de carácter personal.
- Las transferencias de datos que se prevean a países terceros, en su caso.
- La entidad local u órgano de la misma como Responsable del Fichero.
- El servicio, sección, unidad, órgano o cargo donde se puede ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- Las medidas de seguridad, con indicación del nivel básico, medio o alto exigible.

3 Existe un modelo de Ordenanza de creación, modificación o supresión de ficheros en el **Anexo II M6,** así como un modelo de los anexos correspondientes a cada fichero que se deben adjuntar a la Ordenanza en el caso de creación o modificación en el **Anexo II M7.**

4 Cuando una entidad local tenga dudas importantes respecto a la necesidad de crear un fichero y a la forma de realizarlo, podrá solicitar, con carácter previo a la aprobación de la disposición de carácter general, la emisión de un informe por parte de la AVPD. Para ello, puede utilizar el modelo de solicitud que se adjunta en el **Anexo II M8,** al que acompañará el proyecto de norma que quiere aprobar, en su caso, y una memoria con las dudas cuya aclaración solicita.

Cuando una entidad local tenga dudas importantes respecto a la necesidad de crear un fichero y la forma de realizarlo podrá solicitar la emisión de un informe por parte de la AVPD

Artículo 16. Declaración e inscripción de ficheros

Una vez publicada la disposición de creación del fichero en el Boletín del Territorio Histórico, se notificará a la AVPD para su inscripción en el Registro de Protección de Datos. A través de la página Web de la AVPD existe la posibilidad de obtener un programa de auto declaración, así como instrucciones para cumplimentar los formularios. Asimismo, en la misma página, en el Registro de Protección de Datos de Euskadi **se podrán consultar las características de los ficheros creados y declarados por las entidades locales de la CAPV.** El acto de notificación a la AVPD se considerará también notificación a la Agencia Española de Protección de Datos, encargándose la AVPD de trasladar la información a aquella.

3.2. RECOGIDA Y TRATAMIENTO DE DATOS PERSONALES

Artículo 17. Los datos son propiedad de cada persona

1 Las entidades locales de la CAPV tendrán presente, en todo momento, que los datos personales son propiedad de las personas a las que se refieren y que sólo ellas pueden decidir sobre los mismos. La entidad local hará uso de ellos sólo para aquellas finalidades para las que esté facultada debidamente y respetando en todo caso la normativa sobre protección de datos de carácter personal.

Los datos personales son propiedad de las personas a las que se refieren y deberán ser recogidos de forma leal y lícita y tratarse sólo para fines determinados, explícitos y legítimos

2 Los datos de carácter personal deberán ser recogidos de forma leal y lícita, por lo que se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

3 Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas.

Artículo 18. Calidad en la recogida y el tratamiento de los datos personales

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.

Los datos que se soliciten han de ser adecuados, pertinentes y no excesivos para la finalidad para la que se recaban

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

Artículo 19. Mantenimiento y actualización adecuada de los datos personales

1. Los datos de carácter personal serán **exactos y puestos al día,** de forma que respondan con veracidad a la situación actual de la persona afectada. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, inadecuados, incompletos o excesivos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a las personas afectadas reconocen el artículo 8 y siguientes de la LOPD.

2. 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 o se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recabados.

Artículo 20. Consentimiento de la persona

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

2 **No será preciso el consentimiento previo** cuando:

- **Exista una ley que así lo disponga** y, en consecuencia, los datos de carácter personal se recojan para el ejercicio de las funciones propias de la entidad local actuante en el ámbito de sus competencias, ni cuando exista un contrato o relación de negocio, laboral o administrativa, y tales datos sean necesarios para su mantenimiento o cumplimiento.
- **La finalidad del tratamiento de los datos sea proteger un interés vital de la persona interesada,** como la prevención, el diagnóstico o el tratamiento médico, la prestación de asistencia o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por personal sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.
- **Los datos figuren en fuentes accesibles al público** y su tratamiento sea necesario para la satisfacción de un interés legítimo perseguido por la entidad local, por la persona Responsable del Fichero y por la persona destinataria de los datos, siempre que no se vulneren los derechos y libertades fundamentales de la persona interesada.

3 Los ciudadanos y ciudadanas tienen **derecho a no dar el consentimiento cuando sea preceptiva su autorización.**

4 **El consentimiento podrá ser revocado** cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. La revocación del consentimiento deberá realizarse necesariamente mediante escrito dirigido a la persona Responsable del Fichero, manifestando tal decisión y ésta deberá responder en el plazo de 10 días naturales, contados a partir del día siguiente al de la recepción de la solicitud de revocación del consentimiento, materializando, en su caso, tal revocación dentro del mismo plazo. Si los datos para cuyo tratamiento se revoca el consentimiento hubieran sido comunicados previamente, la entidad local actuante deberá notificar la revocación del consentimiento efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último.

5 Existen modelos de formulario para dar el consentimiento expreso en el **Anexo II M9,** así como para revocarlo en el **Anexo II M10.**

Artículo 21. Recogida de datos especialmente protegidos

1 Respecto a los **datos personales relativos a la salud,** éstos sólo podrán ser recabados y tratados cuando por razones de interés general así lo disponga una ley o cuando la persona interesada consienta expresamente. El personal al servicio de la entidad local directamente relacionado con la salud de los trabajadores y trabajadoras podrá tratar los datos de carácter personal relativos a la salud de las personas que atiendan, de acuerdo con lo dispuesto en la normativa vigente en materia de sanidad y de protección de la salud y prevención de riesgos laborales.

2 El tratamiento de datos relativos a ideología, religión, creencias y afiliación sindical, requiere el consentimiento expreso y por escrito de la persona interesada. Los **datos** de carácter personal **que se refieran a la vida sexual, salud u origen racial** de las personas sólo serán recabados, tratados y cedidos cuando por razones de interés público así lo establezca una ley o la persona interesada consienta expresamente. En el caso en que se recaben datos relativos a la ideología, religión o creencias de la persona interesada, ésta será advertida de su derecho a no consentir el tratamiento de tales datos.

Necesidad de consentimiento expreso y por escrito para recabar datos relativos a la ideología, religión, creencias y afiliación sindical de la persona

3.3. RESPECTO DE LOS DERECHOS DE LAS PERSONAS

Artículo 22. Facilitar a las personas el ejercicio de sus derechos

1 La entidad local no sólo permitirá sino que facilitará a las personas el ejercicio de los derechos enumerados en los artículos 6 y siguientes. A este efecto creará los procedimientos administrativos oportunos para que se puedan ejercer fácilmente los derechos de acceso, rectificación, cancelación y oposición.

2 Así, **la entidad local se compromete a:**

- **Arbitrar un procedimiento específico para facilitar el ejercicio de estos derechos.** Se adjuntan como **Anexo III P1.1** una descripción del procedimiento y como **Anexo III P1.2** un esquema del procedimiento. Este procedimiento, en su caso, se podrá adecuar en la forma que en cada caso se estime más conveniente.

- **Poner a disposición de la ciudadanía modelos para el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición,** que estarán a disposición de las personas interesadas bien en el Registro General, en el Servicio de Información o Atención Ciudadana, bien en cualquier otra dependencia donde se realice el tratamiento, así como en la página Web de la entidad local. En este sentido se utilizarán los modelos del **Anexo II M2, M3, M4 y M5,** donde se incluye información sobre las normas de aplicación y las condiciones y plazos para su ejercicio, tramitación y atención.

- **Informar y formar adecuadamente al personal** que tenga acceso a los datos del fichero para que puedan atender adecuadamente a la ciudadanía en el ejercicio de sus derechos.

- Incorporar progresivamente en los nuevos aplicativos informáticos las funcionalidades que faciliten el ejercicio de los derechos de acceso, rectificación, cancelación u oposición, con el objeto de permitir a las personas interesadas la identificación de los procedimientos para el ejercicio de sus derechos.

3.4. EN SUS RELACIONES CON TERCERAS PERSONAS O ENTIDADES

Artículo 23. Contratación para la prestación de servicios que conlleven acceder a datos personales

23.1. Encargo de un servicio que implica el acceso a datos personales de ficheros de la entidad local

1 Cuando la entidad local facilite el acceso a datos personales a una tercera persona o entidad para que realice un tratamiento concreto con ellos por encargo de la propia administración, no se considerará comunicación de datos.

2 Independientemente del coste de la prestación del servicio, la entidad local regulará la realización del tratamiento con la parte prestataria, preferentemente mediante **contrato** por escrito, o en cualquier otra forma, siempre que permita acreditar su celebración y contenido, estableciéndose expresamente:

- **OBJETIVO**

- Qué datos o categorías de datos se facilitan o **a qué datos se posibilita el acceso a la empresa contratada**.
- En qué **fichero** está contemplado su tratamiento (denominación, disposición de carácter general que lo crea, etc.).
- Para qué **tipo de actividad** o actividades o finalidad se concreta el trabajo.
- **Cómo deben tratarse los datos** (con el mayor detalle posible).

Cuando la entidad local facilite datos personales a una tercera persona o entidad para un tratamiento concreto, deberá formalizar un contrato por escrito

OBLIGACIONES PARA LA EMPRESA O ENTIDAD PRESTATARIA

- Asumir la obligación genérica de **cumplimiento** de lo dispuesto en la **Ley Orgánica 15/1999,** de 13 de diciembre, de Protección de Datos de Carácter Personal y, expresamente, en lo indicado en su artículos 9 y 10, y en el Reglamento de desarrollo de la citada Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, comprometiéndose explícitamente a **informar y formar a su personal** en las obligaciones que de tales normas dimanan.

- **Utilizar la información** y datos de carácter personal que se le faciliten única y **exclusivamente para la finalidad** de realización de las actividades contempladas en el contrato de cesión de datos.

- Tratar la información conforme a las instrucciones que consten o que se trasladen posteriormente.

- **Guardar el secreto profesional,** tanto la empresa como el personal a su cargo, sobre todas las informaciones, documentos y asuntos a los que tenga acceso o conocimiento durante la vigencia del contrato, estando obligados a no hacer públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo contractual.

- **Cumplir las medidas de seguridad** y adoptar las medidas necesarias de índole técnica y organizativa que garanticen la seguridad de los datos personales que se le faciliten, conforme al nivel de seguridad del fichero de que se trate, de tal manera que 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 de medio físico o natural.

La empresa contratada está obligada a no reproducir, ni comunicar, ni ceder a terceras personas o entidades información a la que tengan acceso durante la ejecución del contrato

- **Poseer un Documento de Seguridad formalizado y documentado,** en el que se determinen las medidas de índole técnica y organizativa que deben implementarse atendiendo a la naturaleza de los datos. A tal fin, la parte adjudicataria deberá aportar con anterioridad a que se produzca la cesión de datos, en su caso, una memoria descriptiva de las medidas que adoptará para asegurar la confidencialidad e integridad de los datos manejados y de la documentación facilitada, con indicación asimismo del nombre de la persona Responsable de la Seguridad en su empresa de esos datos y tratamientos, con especificación de su perfil profesional.

OBLIGACIONES PARA LA EMPRESA O ENTIDAD PRESTATARIA

- **Informar a la entidad local** contratante, de modo inmediato, sobre cualquier sospecha relacionada con fallos o fugas del sistema de seguridad y protección de la información que pudiera ser detectado durante la ejecución del contrato.

- Facilitar, en su caso, el control y auditoría por parte de la entidad local contratante, mediante la aportación de la información que se le solicite e incluso, excepcionalmente, el acceso a los locales que se determinen. Incluso autorizar a la entidad local la posibilidad de utilizar registros de control en los ficheros facilitados.

- **No reproducir, ni comunicar, ni ceder a terceras personas la información** suministrada o de la que tenga conocimiento durante la ejecución del contrato.

- **No subcontratar la actividad,** en todo o en parte, **sin autorización expresa para ello.** En este supuesto deberán recogerse por escrito los datos que podrán facilitarse por la empresa adjudicataria a la empresa subcontratista y todas las obligaciones de ésta última, que serán como mínimo las de aquella, respecto de la administración contratante.

- Borrar los datos o devolver el soporte informático en el que constan los datos personales que provienen de los ficheros que se le han facilitado, una vez prestados los servicios requeridos, sin conservar copia alguna del mismo, ni siquiera de seguridad, y sin que ninguna persona externa, física o jurídica, entre en conocimiento de los datos. Asimismo devolverá o destruirá todos los soportes magnéticos, soportes ópticos o cualquier otro tipo de soporte procesable.

Una vez finalizados los servicios requeridos, la empresa contratada está obligada a borrar los datos sin conservar copia de los mismos

OBLIGACIONES PARA LA EMPRESA O ENTIDAD PRESTATARIA

- Si la parte adjudicataria aporta equipos informáticos, una vez finalizadas las tareas y previamente a retirar dichos equipos, deberá borrar toda la información utilizada o que se derive de la ejecución del contrato, mediante un sistema que impida su recuperación. La destrucción de la documentación de apoyo se efectuará mediante máquina destructora de papel o cualquier otro medio que garantice la ilegibilidad, realizándose esta operación en el lugar donde se realicen los trabajos.

- En el caso de que la empresa o la persona designada por la misma para realizar el tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerada también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

3 Con la finalidad de asegurar el cumplimiento de las prescripciones contempladas en este apartado, **en los pliegos de cláusulas administrativas generales o de condiciones técnicas, se recogerán las anteriores obligaciones** para que sean asumidas por las personas participantes en los procedimientos de contratación administrativa.

4 Existe un modelo de formulario para este clausulado en el **Anexo II M11.**

23.2. Encargo a una tercera persona o entidad de un servicio, en cumplimiento del cual pudiera tener acceso a datos de carácter personal de la administración

1 Será necesario recoger en el contrato escrito que suscriban ambas partes, al menos, las cláusulas referidas a:

- Acceso a locales donde se tratan datos personales.
- Deber de confidencialidad de las personas que accedan a datos de carácter personal.
- Cumplimiento de medidas de seguridad por parte de esas mismas personas.

2 Existe un modelo de formulario para este clausulado en el **Anexo II M12**.

3.5. MEDIDAS DE SEGURIDAD DE LOS FICHEROS

Artículo 24. Tipos de fichero y niveles de seguridad

1 El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, establece los tres niveles de seguridad -básico, medio y alto-, que se deben aplicar a los ficheros y tratamientos en función de la naturaleza de los datos personales que contienen. Concretamente, determina lo siguiente:

Deberán reunir medidas de seguridad de nivel alto todos los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual, así como los que tengan fines policiales, sin el consentimiento de las personas afectadas y los que contengan datos derivados de actos de violencia de género

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

- Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, los de Administraciones tributarias, los de servicios financieros, aquellos ficheros destinados a prestación de servicios de información sobre solvencia patrimonial y crédito, los de las Entidades Gestoras y Servicios Comunes de la Seguridad Social, los de las mutuas de accidentes de trabajo y aquellos que permitan evaluar la personalidad deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.

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

2. Se adjunta como **Anexo IV D5** un cuadro explicativo de los distintos niveles de seguridad y las medidas aplicables a cada uno de ellos.

Artículo 25. Funciones y obligaciones de las personas que tratan datos de carácter personal

1. Todo el personal al servicio de una entidad local que realice tratamientos de datos de carácter personal, de forma general o excepcional, deberá respetar la legislación y normativa aplicable al respecto, para lo que deberán aplicar de manera diligente lo establecido en la mencionada normativa y en el presente Manual de Buenas Prácticas.

2. **Quienes tengan personas bajo su responsabilidad deberán formarlas** debidamente en sus deberes y obligaciones respecto al tratamiento y protección de datos de carácter personal, prestando especial atención a la formación en la fase de acogida, cuando se incorporen por primera vez a sus equipos.

Todas las personas al servicio de una entidad local deberán respetar la legislación en materia de protección de datos

3. En función de la estructura de cada entidad local, que asume su responsabilidad corporativa en relación con su deber de garantizar una protección de datos de carácter personal eficaz y válida en su ámbito, se identifican las siguientes figuras, como potenciales agentes en la protección de datos de carácter personal en cada organización:

a) La persona que presida la entidad local asumirá la máxima responsabilidad de la efectiva aplicación de dicha legislación y normativa.

b) Responsable del Fichero: la **entidad local** se constituye como responsable última de todos los ficheros que contengan datos de carácter personal en sus instalaciones. Asimismo, le corresponde decidir sobre la finalidad, contenido y uso del tratamiento de datos de carácter personal. Para la realización de tareas operativas relacionadas con la seguridad de los ficheros la Presidencia de cada entidad local designará, en caso de que delegue en otra, a la persona física que, de entre su personal, deba realizar las tareas de control de uno o varios ficheros, sin que dicha delegación de actividades suponga una exoneración de las responsabilidades que, en materia de seguridad de datos de carácter personal, corresponde a la administración.

c) Responsable de Seguridad: persona encargada de definir y velar por el cumplimiento de la estrategia global en materia de seguridad de la información en la administración y, especialmente, la correcta adecuación de la misma a lo establecido en la legislación y normativa relativa a la protección de datos de carácter personal. Tiene atribuidas por la persona Responsable del Fichero la función de coordinar y controlar las medidas de seguridad aplicables. En el ejercicio de sus competencias podrá recabar la colaboración de la persona que en cada administración tenga atribuida la función de asesoramiento legal, a fin de asegurar la idoneidad de las propuestas o acciones que se deban realizar, en el ámbito jurídico.

d) Comisión para la protección de datos personales: órgano que con carácter consultivo y de apoyo a la toma de decisiones en materia de seguridad de la información y protección de datos de carácter personal puede constituirse en cada entidad local, con la composición y régimen de funcionamiento que se estime más conveniente, habida cuenta de las características funcionales, tamaño y complejidad orgánica de cada entidad local.

e) Usuario/a: persona o proceso autorizado para acceder a datos o recursos.

f) Persona o entidad Encargada del tratamiento: persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta de una entidad local. Cabe la posibilidad de que la entidad local contrate la asistencia técnica necesaria para llevar a cabo tratamientos puntuales de la información.

g) Persona colaboradora o coordinadora en materia de protección de datos: persona que pueden designar las entidades locales con el encargo de coordinar, dinamizar y extender la nueva cultura de la protección de datos. Podrá coincidir o no con alguna de las figuras anteriores.

Artículo 26. Documento de Seguridad

1. La entidad local implantará la normativa de seguridad mediante un Documento de obligado cumplimiento para el personal con acceso a los datos de carácter personal y a los sistemas de información.

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

- Ámbito de aplicación del Documento, con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en la normativa vigente y en este Manual de Buenas Prácticas.
- Funciones y obligaciones del personal.
- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.

Todos los ayuntamientos deberán redactar un documento de seguridad

- Procedimientos de realización de copias de respaldo y de recuperación de los datos.

- Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio Documento de Seguridad.

- Medidas a adoptar cuando un soporte o documento vaya a ser transportado, desechado o reutilizado.

3. **El Documento deberá mantenerse actualizado en todo momento** 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.

5. Se adjunta como **Anexo IV** un Documento de Seguridad que podrá utilizarse por las administraciones como modelo.

Artículo 27. Comunicación de sus obligaciones a las personas con acceso a datos

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.

2. La persona 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 28. Sistemas de identificación y autenticación

1. La persona Responsable del Fichero se encargará de que exista una relación actualizada de personas que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.

Deberá establecerse un proceso de identificación y autenticación para evitar accesos no autorizados

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.

4. Se establecerá un mecanismo que permita la **identificación** de forma inequívoca y personalizada **de toda persona usuaria que intente acceder al sistema de información** y la verificación de que está autorizada para tal fin.

5. Las personas usuarias serán siempre personas físicas, identificadas unívocamente, no permitiéndose los accesos de personas usuarias mediante cuentas o identificativos compartidos. **Cada persona usuaria será responsable de todas las actuaciones que se realicen con su identificativo.**

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

Artículo 29. Control de acceso a aplicaciones informáticas

1. Las personas usuarias tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. Se establecerán mecanismos para evitar que una persona usuaria pueda acceder a datos o recursos con derechos distintos de los autorizados.

2. La relación de personas usuarias, a la que se refiere el artículo anterior de este Manual de Buenas Prácticas, contendrá el acceso autorizado para cada una de ellas. **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 en el Documento de Seguridad.

Las personas usuarias sólo tendrán acceso autorizado a los datos y recursos que sean necesarios para el cumplimiento de sus funciones

Artículo 30. Registro de accesos en ficheros de nivel alto

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

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

3. Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo de la persona Responsable de Seguridad, sin que se deba permitir, en ningún caso, la desactivación ni la manipulación de los mismos.

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

5 La persona Responsable de Seguridad se encargará de **revisar periódicamente la información de control registrada y elaborará un informe** de las revisiones realizadas y de los problemas detectados, al menos una vez al mes.

Artículo 31. Acceso a locales donde estén ubicados los equipos con la información

1 Solamente 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.

2 Los locales donde estén ubicados los **sistemas de información de nivel alto** deberán estar dotados de un sistema de control de accesos que permita el acceso sólo a las personas autorizadas, disponiendo en todo momento de un **registro de las personas y accesos realizados.**

Artículo 32. Acceso a datos a través de la red

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 sea manipulada por terceras personas.

Para transmitir datos da carácter personal de forma electrónica será necesario cifrarlos o encriptarlos

Artículo 33. Régimen de trabajo en estaciones de trabajo y portátiles

La ejecución de tratamientos de datos de carácter personal fuera de los sistemas informáticos de la entidad local, desde estaciones de trabajo o equipos portátiles particulares o propiedad de la entidad local, deberá ser autorizada expresamente por la persona Responsable del Fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado y su cifrado.

Artículo 34. Gestión de soportes

1. Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen solo a aquellos usuarios y usuarias con acceso autorizado y deberán ser inventariados y etiquetarse para almacenarse en un lugar con acceso restringido al personal autorizado para ello en el Documento de Seguridad.

Se debe autorizar la salida de datos personales en equipos portátiles u otros soportes

2. Al margen de lo establecido en el artículo 35.4, 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 la persona Responsable del Fichero.

3. 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, la persona emisora, 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.

4. 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, la persona destinataria, 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.

5 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.

6 Cuando los soportes se vayan a distribuir o vayan a salir fuera de los locales en que se encuentren ubicados los ficheros, como consecuencia de operaciones de mantenimiento, salvaguarda o de necesidades de trabajo, se adoptarán las medidas pertinentes encaminadas a evitar cualquier manipulación indebida de la información almacenada.

Artículo 35. Copias de respaldo y recuperación de los datos

1 La persona Responsable de fichero o, por delegación, la persona Responsable de Seguridad, 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 de los ficheros, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

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

Deberá realizarse una copia de respaldo y conservarse en un lugar diferente de aquél en que se encuentren los equipos informáticos que tratan los datos personales

Artículo 36. Ficheros temporales, copias de trabajo de documentos y pruebas con datos reales

1. Los ficheros temporales o copias de documentos que se hubieran creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda, con arreglo a la naturaleza de la información y, en su caso, de las finalidades de los mismos, en relación con la mayor o menor necesidad de garantizar la confidencialidad, integridad y disponibilidad de la información.

Los ficheros temporales o copias de trabajo se borrarán cuando dejen de ser necesarios

2. Todo fichero temporal o copia de trabajo así creado será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.

3. 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.

Artículo 37. Registro de incidencias

1. 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.

2. Se deberán consignar en este registro 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.

3. Será necesaria la **autorización por escrito de la persona Responsable del Fichero para la ejecución de los procedimientos de recuperación de los datos.**

Artículo 38. Circuito de datos en soporte papel y destrucción de copias

1. **Cuando** para la tarea de gestión **sea necesario utilizar listados o copias impresas en papel que contengan datos personales** se establecerá un sistema para que sólo las personas usuarias autorizadas tengan acceso a su contenido y **evitar que la información sea accesible por personas no autorizadas.**

2. En el supuesto de que sea necesario que la información en papel salga fuera de los locales administrativos se adoptarán las medidas necesarias para evitar un uso indebido de la misma.

3. Cuando los listados o copias impresas en papel dejen de ser necesarias se adoptarán las medidas necesarias para su destrucción.

Artículo 39. Auditorías

1. Los sistemas de información e instalaciones de tratamiento de datos se someterán a una **auditoría interna o externa bianual,** que verifique el cumplimiento del presente Manual de Buenas Prácticas y de los procedimientos e instrucciones vigentes en materia de seguridad de datos.

2 El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Manual de Buenas Prácticas, y a la reglamentación vigente relativa a protección de datos de carácter personal, 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, en su caso, por la persona Responsable de Seguridad, quien comunicará las conclusiones a cada persona Responsable del Fichero para que se adopten las medidas correctoras adecuadas. Los informes de auditoría realizados quedarán a disposición de la AVPD.

Será necesario realizar auditorías sobre las medidas de seguridad para identificar deficiencias y medidas protectoras

Artículo 40. Actuaciones respecto a ficheros no automatizados

40.1. Actuaciones respecto a ficheros no automatizados de nivel básico

1 Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de **mecanismos que obstaculicen su apertura.** Igualmente se deberá identificar el tipo de información que contienen, ser inventariados y almacenarse en lugares controlados por el personal autorizado para ello en el Documento de Seguridad.

2 La persona Responsable del Fichero deberá establecer los **procedimientos** que deban seguirse en el **archivo de los ficheros no automatizados.** Dichos procedimientos estarán dirigidos a garantizar la correcta conservación de los documentos, la localización y consulta de la información y a posibilitar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3 Mientras la **información no se encuentre en el archivo,** por estar en revisión o tramitación, la persona que se encuentre a cargo de ella deberá **custodiarla** e impedir el acceso a la misma de personas no autorizadas.

40.2. Actuaciones respecto a ficheros no automatizados de nivel medio

1 Existirá para estos ficheros una persona Responsable de Seguridad con las mismas responsabilidades y funciones que para los ficheros automatizados.

2 Estos ficheros se someterán a una auditoria interna o externa al menos cada dos años.

40.3. Actuaciones respecto a ficheros no automatizados de nivel alto

1 El acceso a la documentación se limitará al personal autorizado en el documento de seguridad. Cuando existan múltiples, deberán establecerse mecanismos que permitan identificar los accesos.

2 El local en que se encuentre el fichero deberá estar dotado de **puertas con llave o dispositivo equivalente,** debiendo estar cerradas cuando no sea preciso el acceso a los documentos. Si ello no fuera posible, la persona Responsable de Seguridad hará un informe motivado proponiendo alternativas. En cualquier caso, los armarios, archivadores o elementos de almacenamiento deben tener sistemas que obstaculicen el acceso no autorizado.

3 La copia de documentos sólo podrá ser realizada por personal autorizado. Cuando se destruyan las copias, se hará mediante procedimientos que impidan su posterior recuperación.

4 En el traslado de estos ficheros deberán adoptarse medidas de seguridad que impidan el acceso a la documentación de personas no autorizadas, o la manipulación de la información o la detección de accesos no autorizados.

3.6. CESIÓN O COMUNICACIÓN DE DATOS DE CARÁCTER PERSONAL

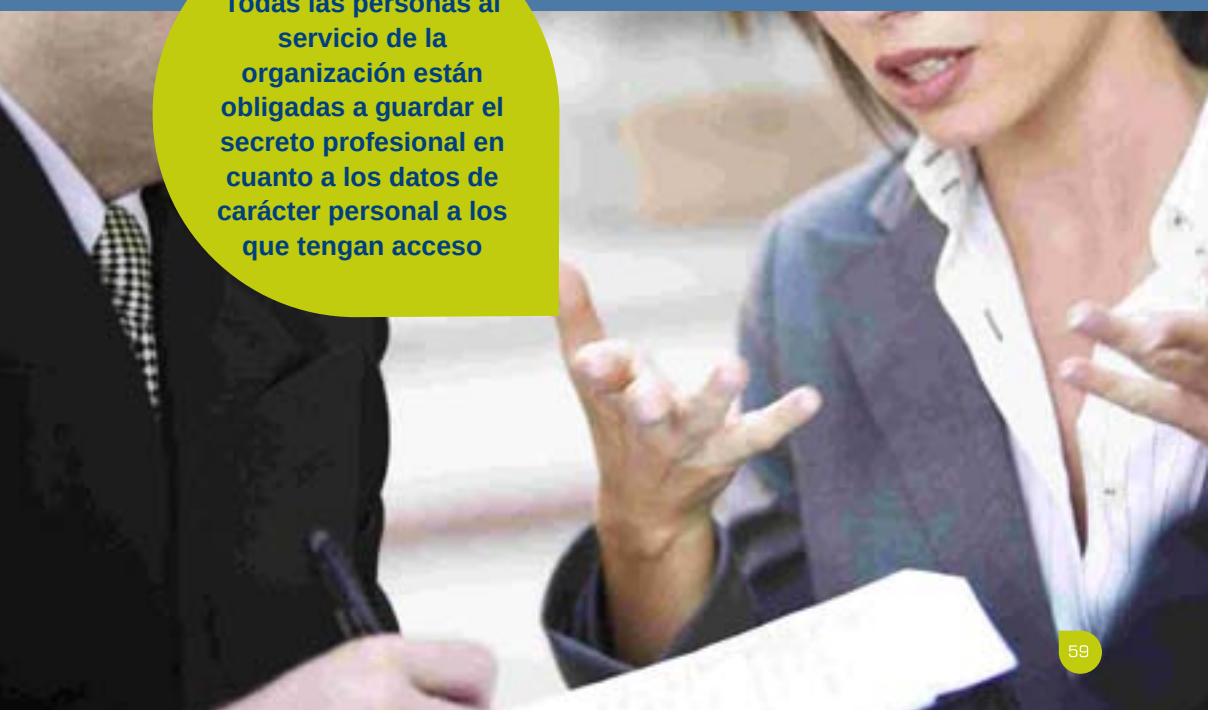
Artículo 41. Deber de secreto profesional

1. Toda persona que intervenga en cualquier fase del tratamiento de los datos de carácter personal de ficheros está obligada al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar su relación de servicio con la entidad local.

2. **El incumplimiento del deber de secreto será sancionado** de conformidad con lo previsto en la legislación vigente y traerá consigo, en su caso, las responsabilidades penales, disciplinarias y ante terceras personas o entidades que la misma establece.

3. Se adjunta como **Anexo II M13** un modelo de carta que las entidades locales podrán enviar a su personal recordándole el deber de secreto y las consecuencias de su inobservancia.

Todas las personas al servicio de la organización están obligadas a guardar el secreto profesional en cuanto a los datos de carácter personal a los que tengan acceso



Artículo 42. Obligaciones en las comunicaciones de datos

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a una tercera persona **para el cumplimiento de fines directamente relacionados** con las funciones legítimas de la entidad local y de la parte cesionaria, así como **con el previo consentimiento** de la persona interesada.

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

- Cuando **la cesión está autorizada en una ley.**
- Cuando se trate de datos recogidos de **fuentes accesibles al público.**
- 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 terceras personas o entidades. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

Será necesario el consentimiento previo de la persona afectada para ceder datos a terceras personas o entidades, excepto en los casos contemplados por la Ley

- Cuando la comunicación que deba efectuarse tenga por **destinatario al Defensor o la Defensora del Pueblo, al Ararteko, al Ministerio Fiscal o a los jueces y juezas o tribunales o al Tribunal Vasco de Cuentas,** en el ejercicio de las funciones que tienen atribuidas.
- Cuando la cesión se produzca entre administraciones públicas y tenga por objeto el tratamiento posterior de los datos con **fines históricos, estadísticos o científicos.**

- **Cuando los datos** hayan sido recogidos o elaborados **por una administración pública con destino a otra,** o cuando se realice para el **ejercicio de competencias sobre las mismas materias.**

- 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 una tercera persona, cuando la información que se facilite a la persona interesada no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

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

5 Aquella persona 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 LOPD.

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

7 Se adjunta como **Anexo II M14** un modelo de autorización de la cesión de datos, y como **Anexo III P2** un esquema del procedimiento de actuación ante peticiones de cesión de información.

Artículo 43. Procedimiento para las cesiones de datos que requieran el consentimiento de la persona interesada

1. En el caso de cesiones de datos que precisen del consentimiento de la persona interesada, tanto a entidades de derecho público como a entidades de derecho privado, se procederá de la siguiente forma:

   - **Las entidades solicitantes remitirán su petición a la persona Responsable del Fichero,** que valorará la oportunidad de la cesión así como su legalidad, sin perjuicio de que pueda recabar el asesoramiento jurídico de quien tenga atribuida dicha función en cada entidad local.

   La persona Responsable del Fichero comprobará la autorización prestada por las personas afectadas

   - La persona Responsable del Fichero remitirá la **carta de condiciones** a la entidad solicitante para que la firme mediante «recibí y conforme».

   - La persona Responsable del Fichero comprobará la autorización prestada por las personas afectadas, debiendo solicitarles expresamente su consentimiento si fuera necesario, y llevará a cabo un sistema de marcado en las fichas personales generadas al efecto, donde consten en cada momento las cesiones realizadas, a fin de garantizar el efectivo ejercicio de los derechos de acceso, rectificación y cancelación de las personas interesadas.

   - La persona Responsable del Fichero comunicará los datos a la parte cesionaria en el soporte que se determine. Las cesiones realizadas serán reflejadas en el correspondiente registro de entradas y salidas del Documento de Seguridad del fichero.

2. Se adjunta en **Anexo II M15** las cláusulas que deben ser asumidas en todo caso por las personas cesionarias de datos cuando se realicen cesiones de datos que requieran consentimiento de la persona interesada, en adelante, la Carta de Condiciones a aceptar por la parte cesionaria.

Artículo 44. Procedimiento para las cesiones de datos que no requieran el consentimiento de la persona interesada

1. En el caso de cesiones de datos que no precisen del consentimiento de la persona interesada de acuerdo con lo previsto en el artículo 42.2, tales cesiones se llevarán a cabo mediante la supervisión de la persona Responsable del Fichero. Algunos ejemplos de cesiones de este tipo son:

   - **La cesión realizada a organismos judiciales y administrativos,** de conformidad con las diferentes leyes aplicables, en el ejercicio de las funciones que tienen atribuidas y en los supuestos y condiciones establecidos en las citadas normas.

   - La cesión de datos personales pertenecientes a empleados y empleadas de la entidad local realizada **a quienes ostenten su representación sindical,** en cumplimiento de la Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical, y de la Ley 2/1991, de 7 de enero, sobre derecho de información de los representantes de los trabajadores en materia de contratación o normativa vigente en cada momento.

   - **Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia** que requiera acceder a un fichero automatizado, o para realizar los estudios epidemiológicos en los términos establecidos en la Ley 14/1986, de 25 de abril, General de Sanidad, y sus disposiciones complementarias, en la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales o en la normativa vigente en cada momento.

   - **Cuando** la cesión se efectúe previo procedimiento de disociación, es decir, de modo que **la información que se obtenga no pueda asociarse a persona determinada o determinable.**

2. Sin perjuicio de lo anterior, y dada su especialidad, las cesiones de datos para la prestación de servicios de acuerdo con lo dispuesto en el artículo 12 de la LOPD, seguirán la tramitación prevista en el artículo 22 de este Manual.

Artículo 45. Utilización y tratamiento de datos del Padrón Municipal de Habitantes

45.1. Finalidad del Padrón Municipal de Habitantes

Las finalidades para las que se pueden utilizar los datos del Padrón Municipal de Habitantes son, exclusivamente, las establecidas al efecto en la Ley Reguladora de las Bases del Régimen Local:

- Determinar la población del municipio (15 LRBRL).
- Constituir prueba de la residencia en el municipio y del domicilio habitual en el mismo (16.1 LRBRL).
- Elaborar estadísticas (16.3 LRBRL) sobre composición de familias, características económicas, nivel educativo, matrimonio, fecundidad y defunciones.

45.2. Cesión a otras administraciones sin consentimiento previo por tener la consideración de cesiones legales

Los datos del Padrón Municipal se cederán a otras administraciones sin consentimiento previo, para el ejercicio de sus competencias, cuando la residencia o domicilio sea un dato relevante

Los datos del Padrón Municipal de Habitantes se cederán a otras administraciones públicas que lo soliciten, **sin consentimiento** previo de la persona afectada solamente cuando les sean necesarios para el ejercicio de las respectivas competencias de ambas administraciones, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes.

En este sentido, la administración peticionaria deberá justificar ante la entidad local requerida la función que se propone realizar con los datos padronales, debiéndose acreditar la relevancia de la residencia o el domicilio y, además, deberá encuadrar dicha función en alguna de las competencias que le reconoce el ordenamiento jurídico, indicándola expresamente en su petición.

Una vez acreditada y justificada la petición se podrá acceder a la misma y **se cederán los datos del Padrón Municipal de Habitantes que sean adecuados, pertinentes y no excesivos** para el cumplimiento de la competencia legítima atribuida a la administración pública peticionaria.

45.3. Otras cesiones de datos del Padrón Municipal de Habitantes sin consentimiento de la persona afectada

1. Por disposición expresa de la legislación vigente aplicable a este efecto, **los datos del Padrón Municipal de Habitantes se cederán a requerimiento de las instituciones siguientes:**

   - **A las Fuerzas y Cuerpos de Seguridad para fines policiales** cuando su finalidad sea la prevención de un peligro real para la seguridad pública o la represión de infracciones penales.
   - **A la Administración Tributaria.**
   - Al Defensor o la Defensora del Pueblo, Ararteko, Ministerio Fiscal, jueces o juezas, tribunales y Tribunal Vasco de Cuentas.

2. **También pueden cederse dichos datos para elaborar estadísticas oficiales sometidas al secreto estadístico,** en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, y en la Ley 4/1986, de 23 de abril, de Estadística de la Comunidad Autónoma de Euskadi.

3. Fuera de estos supuestos, los datos del Padrón Municipal de Habitantes son confidenciales y el acceso a los mismos se regirá por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

45.4. Cesión de datos interdepartamental

1. Si bien ni la LOPD ni la Ley 2/2004 hablan de cesión de datos entre órganos de una misma entidad local, ello no puede significar que los prohíba y que los requisitos para dicha cesión, debe entenderse, sean los mismos que los previstos para la cesión entre administraciones públicas.

2. En consecuencia, cuando la cesión de datos del Padrón Municipal de Habitantes sea para el ejercicio de una competencia que corresponde a la propia entidad local, en la que el domicilio sea dato relevante, no existirá problema para dicha comunicación sin consentimiento de la persona interesada. Cuando concurra dicha circunstancia habrá de entenderse que existe compatibilidad de fines.

3. **No ocurrirá lo mismo cuando los datos se cedan desde otros ficheros que no sean el del Padrón Municipal de Habitantes.** En consecuencia, no podrá admitirse el uso compartido de los datos de un fichero en el que se recojan datos de carácter personal para la tramitación de un expediente administrativo, ni incluso a otro órgano de la propia entidad local, para el desarrollo de una competencia de ésta que no se encuentre expresamente contemplada entre las finalidades del fichero afectado.

Se podrán ceder datos del Padrón Municipal entre departamentos o servicios de una misma entidad local para el ejercicio de una competencia en la que el domicilio sea un dato relevante

4

CONCURRENCIA DEL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL CON OTROS DERECHOS

4.I. DERECHO A LA PROTECCIÓN DE DATOS Y DERECHO DE ACCESO A LA INFORMACIÓN

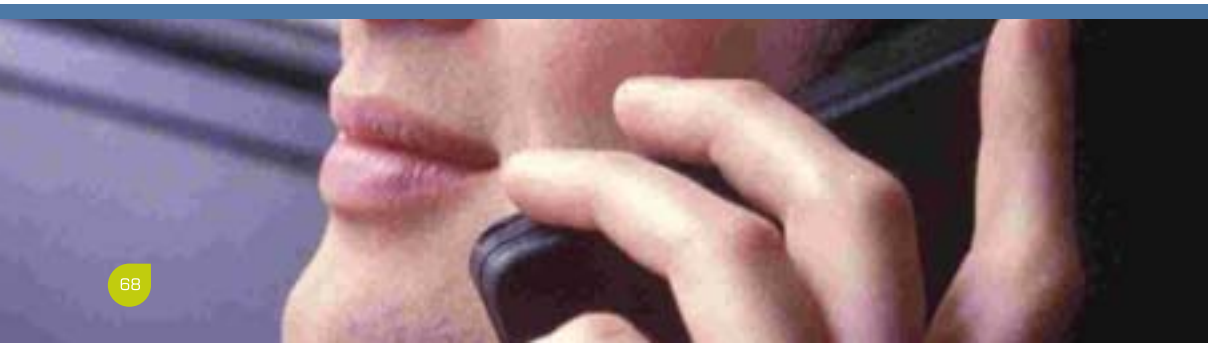
Artículo 46. Del derecho de acceso a la información

1 Está contemplado con carácter general en los artículos 105 b) de la Constitución y en los artículos 35 a), b), g), y h) de la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, así como en la Ley de Bases de Régimen Local y en el Reglamento de Organización y Funcionamiento de las Entidades Locales.

Todas las personas, por el hecho de serlo, tienen el derecho de acceder a la información que existe en las entidades locales

2 El derecho a obtener información de la entidad local corresponde a toda persona por su condición de ciudadana.

3 Toda persona tiene derecho a recibir la información administrativa general contenida en la documentación depositada en los archivos y registros de la entidad local, relativa a: a) la identificación, fines, competencias, estructura, funcionamiento y localización de organismos y unidades administrativas; b) los requisitos jurídicos o técnicos que las disposiciones vigentes impongan a los proyectos, actuaciones o solicitudes que una persona se proponga realizar; c) la tramitación de procedimientos, a los servicios públicos y prestaciones; y d) cualquiera otros datos que las personas interesadas tengan necesidad de conocer en sus relaciones con la entidad local actuante.



Artículo 47. Del ejercicio del derecho de acceso a la información

1. El ejercicio del derecho de acceso a la información y documentación administrativa depositada en los archivos y registros de la entidad local se sujetará a las limitaciones que la Constitución contempla en su artículo 105 b), relativas a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas, y a los principios de proporcionalidad, racionalidad y buena fe a que debe sujetarse el ejercicio de todo derecho, a las del 37.5 de la Ley 30/1992, rigiéndose por disposiciones específicas los accesos contemplados en el 37.6 de la misma.

2. Es objeto del derecho de acceso cualquier documento depositado en los archivos y registros administrativos de entidades locales, cualquiera que sea la forma de expresión gráfica, sonora o en imagen, o el tipo de soporte material en que figure.

3. **El derecho de acceso será ejercido por** las personas de forma que no se vea afectada la eficacia del funcionamiento de los servicios públicos debiéndose, a tal fin, formular **petición individualizada de los documentos que se deseen consultar,** sin que quepa, salvo para su consideración con carácter potestativo, formular solicitud genérica sobre una materia o conjunto de materias. No obstante, cuando quienes lo soliciten sean profesionales de la investigación que acrediten un interés histórico, científico o cultural relevante, se podrá autorizar el acceso directo de aquellos o aquellas a la consulta de los expedientes, siempre que quede garantizada debidamente la intimidad de las personas.

47.1. Acceso a documentación de expedientes en tramitación

El acceso a los **documentos obrantes en los expedientes en trámite se limitará a las personas interesadas o participantes en los procedimientos** afectados, durante el tiempo que dure su tramitación, a fin de preservar la eficacia de la actuación administrativa.

47.2. Acceso a documentación de expedientes terminados

1. Toda persona tiene derecho a obtener copia de los documentos contenidos en los expedientes terminados.

2. No obstante, **cuando se solicite el acceso a los proyectos técnicos** y a la documentación comprensiva de los mismos, presentados para la obtención de las correspondientes licencias, **habrá de ponderarse debidamente su protección, en aras a garantizar el derecho a la propiedad intelectual.**

3. El acceso de las personas a la documentación administrativa contenida en los expedientes terminados tiene su límite en el respeto a la intimidad de las personas.

4. Cuando se facilite información que contenga datos de carácter personal, se procurará que dicha **información se presente de forma disociada,** y si ello no fuera posible, se procederá a asegurar la ilegibilidad de los datos de carácter personal que contenga la documentación a suministrar, mediante su borrado o tachado.

El acceso de cualquier persona a documentación de los expedientes terminados tiene su límite en el respeto a la intimidad de las personas

5 Si una persona solicita el acceso a un expediente terminado que contiene datos personales, se seguirá la práctica de disociación o similar mencionada y sólo a las personas afectadas se facilitará documentación que contenga datos referentes a su intimidad.

6 De manera similar, sólo a las personas afectadas se facilitarán datos nominativos relacionados con expedientes sancionadores y disciplinarios, además de en aquellos otros supuestos contemplados en la ley.

7 Los datos nominativos no íntimos y no relacionados con expedientes sancionadores o disciplinarios se facilitarán a sus titulares y a terceras personas o entidades que acrediten un interés legítimo y directo.

47.3. Denegación del derecho de acceso a la información

En cualquier caso, el ejercicio del derecho de acceso podrá ser denegado cuando prevalezcan **razones de interés público o intereses de tercera persona más dignos de protección** o cuando así lo disponga una ley. La valoración para denegar el acceso corresponde en exclusiva a los correspondientes órganos de la entidad local, ponderando las anteriores circunstancias. En el supuesto de denegación deberá dictarse **resolución motivada.**

Artículo 48. Ejercicio del derecho de acceso por medios electrónicos

1 El principio de transparencia, del que es manifestación esencial el derecho de acceso administrativo, pretende un mejor conocimiento por parte de la ciudadanía de las actividades desarrolladas por la entidad local. Por esta razón, y en base a la Ley 11/2007, de acceso electrónico de la ciudadanía a los Servicios Públicos, la entidad local deberá dotarse de los medios y sistemas electrónicos para que la ciudadanía pueda ejercer su derecho a

comunicarse con las administraciones por medios electrónicos, en la presentación de documentos, en la realización de trámites administrativos, en la consulta de expedientes, la realización de encuestas y, en su caso, en consultas ciudadanas.

2 Cuando la entidad local preste el servicio de acceso a la información por medios electrónicos, velará para que cualquier persona, empresa, administración, institución, organismo o entidad pueda acceder a la máxima información, en lo que se refiere a aspectos generales.

Cuando la entidad local facilite el ejercicio del derecho de acceso a la información por medios electrónicos deberá acreditar suficientemente la identidad de la persona titular del derecho

3 La entidad local adoptará las medidas técnicas necesarias para asegurar que sólo quien sea titular del derecho pueda conocer la información, a cuyos efectos se utilizarán sistemas como la firma electrónica u otros que permitan acreditar suficientemente la identidad del titular o la titular.

4 De la misma manera, deberá asegurarse la práctica de **notificaciones por medios electrónicos,** estableciendo un sistema seguro de comunicación que **garantice la confidencialidad,** evitando la interceptación y alteración de las comunicaciones así como los accesos no autorizados, a través de **mecanismos de autenticación** que garanticen la identidad de la **persona destinataria de la comunicación.**

5 La entidad local podrá publicar en **tablones de edictos virtuales** o en cualquier otra sección de su página Web los actos administrativos cuya notificación no haya podido practicarse personalmente a las personas interesadas, de conformidad con lo dispuesto en el artículo 59.5 LRJPAC.

6 Se adjunta como **Anexo II M16** modelo de contenido de Aviso legal en materia de protección de datos en la Web.

4.2. DERECHO A LA PROTECCIÓN DE DATOS Y PUBLICACIÓN

Artículo 49. Publicidad y difusión de los actos administrativos

1 Con carácter general, cuando deba procederse a la publicación o difusión por cualquier medio de los actos administrativos que deban darse a conocer a las personas interesadas o al público en general, y la información a suministrar contenga **datos de filiación de personas concretas,** se hará referencia a las mismas **mediante las siglas de su nombre y apellidos, evitando, por tanto, su identificación directa.**

2 En general, los boletines y diarios oficiales tienen la consideración de fuentes accesibles al público, por lo que los datos personales allí publicados pueden ser utilizados por terceras personas sin necesidad de solicitar el consentimiento de las personas interesadas, siempre que no se vulneren sus derechos y libertades fundamentales. Por ello, deberá reducirse al mínimo suficiente para cumplir su finalidad la información de carácter personal que se incluya en los documentos a publicar. Asimismo, se podrá **advertir en determinadas publicaciones que los datos personales allí incluidos no podrán emplearse para cualquier finalidad, sino para aquellas determinadas, explícitas y legítimas para las que se hayan publicado.**

Los datos de carácter personal que se publiquen en boletines y diarios oficiales deben reducirse al mínimo suficiente para cumplir su finalidad de información pública

3 La entidad local, ésta podrá ofrecer a la ciudadanía **información sobre el personal a su servicio,** que integre tanto el puesto de trabajo como el número de teléfono y la cuenta de correo electrónico, con el fin de facilitar a la ciudadanía la identidad de la persona con quien deba contactar para realizar una determinada gestión.

Artículo 50. Publicidad en procesos de concurrencia competitiva y protección de datos

1. En los procedimientos de concurrencia competitiva, tales como la selección y provisión de personal al servicio de la entidad local, la concesión de subvenciones, etc., se podrá proceder a la publicación de datos personales relativos a personas físicas identificadas o identificables mediante el empleo de boletines oficiales, tablones de anuncios, medios electrónicos o en la página Web de la propia entidad local, cuando así lo establezcan las **normas reguladoras de cada procedimiento,** a cuyo efecto se deberá contemplar la posibilidad de esta publicación en las bases de selección o en la convocatoria aprobadas.

2. Como medida de cautela, cuando deba procederse a la publicación de datos personales se incluirán **datos disociados o los identificativos mínimos necesarios para cumplir la finalidad de la publicidad requerida.**

En los procedimientos de concurrencia competitiva ha de mencionarse explícitamente la finalidad de los datos personales publicados y que éstos no pueden emplearse para otros fines

3. En cualquier caso, la publicación de información administrativa en los medios mencionados, cuando esta posibilidad venga exigida por la naturaleza de la actuación administrativa, en la medida que constituye un instrumento para el ejercicio de sus competencias, no puede incluirse entre las fuentes de acceso público, por lo que los datos personales que contenga dicha publicación no podrán emplearse para cualquier finalidad, sino para aquellas determinadas, explícitas y legítimas para las que se hayan obtenido. A tal fin, se deberá individualizar con carácter general la finalidad pretendida por la entidad local a la hora de publicar datos de carácter personal.

4.3. DERECHO DE PROTECCIÓN DE DATOS Y DERECHO DE PARTICIPACIÓN POLÍTICA

Artículo 51. Petición de información por miembros de la entidad local y protección de datos

1. Todas las personas que integran una corporación tienen derecho a obtener de la Presidencia de la misma cuantos antecedentes, datos o informaciones obren en poder de los servicios de la entidad local y resulten precisos para el desarrollo de su función de fiscalización y control de los órganos de gobierno de la entidad local, de conformidad con lo establecido en el artículo 77 de la LBRL. En este sentido, el artículo 11.2 a) de la LOPD, en relación con el anterior, ofrece la cobertura suficiente para que a las personas que integran la corporación se les puedan facilitar datos personales.

2. La solicitud del ejercicio del derecho recogido en el párrafo anterior, que deberá reunir los requisitos establecidos en el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Corporaciones Locales, aprobado por Real Decreto 2568/1986, de 28 de noviembre, habrá de ser resuelta motivadamente en los cinco días naturales siguientes a aquel en que se hubiese presentado.

3. Deberán comunicarse sólo aquellos datos de carácter personal que resulten **adecuados, pertinentes y no excesivos** en relación con la concreta finalidad de gobierno o de fiscalización y control que las personas como miembros de la entidad local tengan atribuida.

4. Cuando la información a suministrar contenga datos de carácter personal, se deberá valorar, en primer lugar, **si es posible proceder a su disociación sin que ello afecte al derecho de** los miembros de la entidad local a recibir la información necesaria para el ejercicio de sus funciones de **control de los órganos de gobierno de la entidad local.** Y, cuando esta opción no fuera posible por comprometer la comprensión de la información que deba

suministrarse, se comunicará a quien deba recibir la información el deber de reserva y confidencialidad que le incumbe, respecto de la información de carácter personal que conozca en el ejercicio de su cargo.

5 La valoración de cuáles resulten ser esos datos, así como el cumplimiento de los requisitos de la solicitud y su motivación, corresponde en exclusiva a los correspondientes órganos de gobierno de la entidad local.

Las personas que integran la Corporación tienen el deber de reserva y confidencialidad de la información personal que llegan a conocer al ejercer las responsabilidades de su cargo

6 La comunicación de datos que, en su caso, se realice, deberá encuadrarse dentro de los protocolos que en materia de seguridad tenga establecidos la entidad local, en cumplimiento de los artículos 9 y 20 de la LOPD, en relación con el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

7 Las entidades locales establecerán un procedimiento para el ejercicio de este derecho, que deberá incluir la forma de petición y de contestación y los modelos a utilizar. En el modelo de entrega de documentación, se recordará a las personas que son miembros de la entidad local que deberán observar el **deber de confidencialidad de la información y de los datos de carácter personal** a los que accedan en el ejercicio de su cargo representativo, **aún después de finalizado su mandato.**

Artículo 52. De la publicidad de acuerdos y participación ciudadana en los Plenos de las entidades locales

1. Se deberán facilitar a las personas que lo soliciten **copias y certificaciones acreditativas de los acuerdos de la Corporación;** esta práctica no vulnera la normativa sobre protección de datos de carácter personal **salvo que en dichas copias y certificaciones consten datos de carácter personal especialmente protegidos,** esto es, los contemplados en el artículo 7 de la LOPD. En el resto de supuestos, la comunicación de los datos de carácter personal que obren en dichas copias y certificados, vendría amparada por el artículo 70.3 de la LBRL, en relación con lo dispuesto en el artículo 11.2 a) de la LOPD.

2. También se deberá facilitar a las personas solicitantes una **copia simple del acta,** con el contenido que se expresa en el artículo 229.2 del ROF y, siempre que no afecte a la intimidad de las personas, no vulnerará la normativa sobre protección de datos de carácter personal. En **la exposición pública y resumida de las actas** de los plenos se deben **eliminar aquellos datos personales que resulten excesivos** y no pertinentes para ofrecer información general a la ciudadanía.

3. La exposición pública y resumida de las actas, cualquiera que sea el medio a través del cual se realice, no es contraria a la normativa sobre protección de datos. El "resumen" al que hace referencia dicho precepto aconseja eliminar del mismo aquellos datos de carácter personal que no sean adecuados, pertinentes y resulten excesivos con la finalidad de ofrecer una información "genérica" a los vecinos y vecinas, y en ningún caso debe contener datos de carácter personal sensibles.

4. Cuando se autorice la **grabación** por cualquier medio de las **sesiones que celebre el Pleno** de la entidad local, dicha grabación se suspenderá o se limitará aquella y su difusión, durante el tiempo preciso en el que se traten o debatan asuntos que puedan afectar al derecho a la intimidad personal y familiar.

5

SUPUESTOS CONCRETOS

Artículo 53. Actuación ante supuestos concretos que tienen lugar en las entidades locales respecto del tratamiento de datos de carácter personal

Se adjunta en el **Anexo I** la casuística más relevante y la forma de atenderla respetando las normas de protección de datos de carácter personal. Debido al carácter dinámico de la relación, por la sucesiva aparición de supuestos ahora no contemplados, se ha abordado la estructura de Anexo, más fácilmente actualizable sin alterar esta parte dispositiva.

6

LA AGENCIA VASCA DE PROTECCIÓN DE DATOS

Artículo 54. La Agencia Vasca de Protección de Datos

1 La Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, configura a ésta como 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. En el ejercicio de su actividad, la ley le garantiza plena independencia y objetividad.

La Agencia Vasca de Protección de Datos es una autoridad de control independiente que vela para que las administraciones públicas vascas respeten el derecho de las personas a la protección de sus datos

2 La Agencia Vasca de Protección de Datos asume como **misión** proteger la intimidad personal y familiar de los ciudadanos y ciudadanas, así como el legítimo ejercicio de sus derechos, velando para ello el cumplimiento de la legislación sobre protección de datos.

3 Es, por tanto, una autoridad de control independiente que trabaja para que las administraciones públicas vascas respeten el derecho de las personas a la protección de sus datos personales.

Artículo 55. Actividades de la Agencia Vasca de Protección de Datos

1 La Agencia Vasca de Protección de Datos desempeña, entre otras, las siguientes tareas:

- **INFORMAR Y TUTELAR**

  Informar a las personas acerca de sus derechos y ayudarles en el ejercicio de los mismos mediante la tutela.

- **INVESTIGAR**

  Investigar aquellas actuaciones contrarias a la ley y resolver, en su caso, sobre las infracciones producidas.

- **INSCRIBIR EN EL REGISTRO DE PROTECCIÓN DE DATOS DE EUSKADI**

  Inscribir en el **Registro de Protección de Datos de Euskadi** la relación de los tratamientos de datos personales realizados por las administraciones e instituciones en la Comunidad Autónoma del País Vasco, pero no los datos de cada persona.

- **DAR RESPUESTA A CONSULTAS Y ELABORAR INFORMES SOLICITADOS**

  Dar respuesta a **consultas** y elaborar **informes** que las personas e instituciones soliciten en materia de protección de datos.

- **DIFUNDIR INFORMACIÓN Y GESTIONAR CONOCIMIENTOS Y BUENAS PRÁCTICAS**

  Difundir información, gestionar el conocimiento y buenas prácticas en protección da datos, sensibilizando a la ciudadanía y a las personas al servicio de las instituciones públicas.

7

EL MANUAL Y SU CARÁCTER DE CÓDIGO TIPO

Artículo 56. Código tipo de las entidades locales de la CAPV

1. Este Manual de Buenas Prácticas tiene carácter de Código Tipo de las entidades locales de la CAPV.

2. Este Manual de Buenas Prácticas tiene por objeto adecuar lo establecido en la normativa sobre protección de datos de carácter personal a las peculiaridades de los tratamientos efectuados por las entidades locales de la CAPV y fomentar una mayor concienciación en el campo de la protección de datos de carácter personal entre las entidades locales y las personas que trabajan a su servicio.

El Manual de Buenas Prácticas tiene por objeto adecuar lo establecido en la normativa sobre protección de datos de carácter personal a las peculiaridades de los tratamientos efectuados por las entidades locales de la CAPV

Artículo 57. Entidad promotora, depósito y publicación

1. La Asociación de Municipios Vascos - Euskadiko Udalen Elkartea (en adelante, EUDEL), entre cuyos fines se encuentra la defensa y representación de los intereses generales de los municipios asociados, fórmula y promueve este Manual de Buenas Prácticas.

2. Este Manual de Buenas Prácticas será presentado ante la Agencia Vasca de Protección de Datos, que procederá a su revisión, propondrá, en su caso, adaptaciones legales, y resolverá sobre su inscripción en el Registro de Protección de Datos de Euskadi.

3 EUDEL se responsabilizará de dar suficiente publicidad al Manual de Buenas Prácticas. Por su parte, la AVPD también le dará publicidad a través de su página Web.

4 EUDEL tendrá las siguientes obligaciones:

- **Informar al público a través de su página Web** sobre el contenido del Manual, la actualización de sus anexos, el procedimiento de adhesión y garantía de cumplimiento y la relación de entidades locales adheridas.
- **Informar a la AVPD mediante una memoria anual** sobre las actividades de difusión y promoción del Manual, las de verificación de su cumplimiento, las reclamaciones y quejas tramitadas en relación al mismo y cualquiera otra información que considere relevante.
- **Evaluar periódicamente** la eficacia del Manual y el grado de satisfacción de la ciudadanía con el mismo.
- **Facilitar la accesibilidad a la información** a las personas que tengan alguna discapacidad o dificultad que merme sus posibilidades de acceder a la información.

Artículo 58. Adhesión a este Manual de Buenas Prácticas

1 **Cualquier entidad local de la CAPV podrá adherirse** al presente Manual, siguiendo el siguiente procedimiento:

- Adopción del acuerdo de adhesión y, en su caso, adaptación de los modelos incluidos en los anexos a la relidad específica de cada entidad local.
- Comunicación a EUDEL del acuerdo de adhesión.

2 EUDEL actualizará la lista de entidades locales adheridas, que deberá ponerse a disposición de la AVPD, y será incorporada como **Anexo VI** al Manual transcurridos seis meses desde su inscripción en el Registro.

Artículo 59. Procedimiento de supervisión del cumplimiento de las obligaciones asumidas mediante el acuerdo de adhesión al Manual o Código Tipo

Para **garantizar el cumplimiento de las obligaciones** asumidas por las entidades locales adheridas se establecerá **un procedimiento de supervisión y un régimen sancionador.** A estos efectos se constituirá un grupo de trabajo de entidades locales adheridas que proponga, en los seis primeros meses de vigencia, la regulación de los mencionados procedimientos, que se adjuntarán como anexos al Manual.

Artículo 60. Acciones informativas y formativas en materia de protección de datos

1. Las entidades locales adheridas se comprometen a planificar periódicamente actividades informativas y acciones formativas dirigidas a todo su personal y de manera preferente, a quién trate datos personales y datos sensibles.

2. Asimismo se comprometen a facilitar a su personal un decálogo que informa sobre los principios de la protección de datos, sus obligaciones y los derechos de la ciudadanía. A estos efectos se adjunta como **Anexo II M17** un **Decálogo Tipo.**

Artículo 61. Establecimiento de un *sello de confidencialidad* que identifique a las administraciones adheridas al Manual de Buenas Prácticas

EUDEL coordinará la constitución de un grupo de trabajo de entidades locales adheridas para realizar las siguientes actividades:

- Concretar, en colaboración con la AVPD y con entidades relacionadas con la difusión de la gestión de calidad, la creación de un **sello de confidencialidad** que identifique a las entidades locales adheridas a este Manual.

- Concretar una propuesta de **convocatoria de subvenciones** dirigida a las entidades locales con menos recursos humanos y económicos para la mejora de sus prácticas en materia de protección de datos de carácter personal.

- Concretar una propuesta de convocatoria de implantación de proyectos de adecuación, documentación de procesos y planificación de actividades informativas y acciones formativas dirigida a entidades locales adheridas.

DISPOSICIÓN FINAL. ENTRADA EN VIGOR Y ACTUALIZACIONES

1. Entrada en vigor

Este Manual de Buenas Practicas entrará en vigor en el plazo de dos meses, contado desde su inscripción en el Registro en la Agencia Vasca de Protección de Datos.

2. Actualizaciones y modificaciones

- La **parte dispositiva** del Manual de Buenas Prácticas se **actualizará periódicamente,** a fin de procurar su adaptación progresiva a las innovaciones técnicas y a los cambios legislativos que se produzcan en materia de protección de datos.

- Los anexos serán igualmente actualizados de manera permanente con nuevos supuestos o modelos actualizados.

- EUDEL será la entidad encargada de coordinar las actualizaciones y de notificarlas, tanto a la AVPD como a las entidades locales adheridas.