ANEXO I
SUPUESTOS CONCRETOS

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-1238-08

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

ANEXO I SUPUESTOS CONCRETOS
ÍNDICE

2.2. Acceso a la información. Oficinas de atención a la ciudadanía. Expedición de certificados 79-90

2.8. Gestión de Personas y Datos personales 113-124

ANEXO I

SUPUESTOS CONCRETOS

1. EN GENERAL

1 ¿QUÉ ES EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES?

- Es un derecho fundamental que surge con el desarrollo de las nuevas tecnologías de la información y la comunicación.
- Debe considerarse como parte de una cuestión más amplia: la de la protección de la vida privada y la dignidad humana. Así, algunas personas lo incluyen en el ámbito de los derechos humanos de tercera generación, es decir, el derecho a la identidad del individuo, a la propiedad sobre la propia información y el derecho a la intimidad, a la privacidad y a la propia imagen.
- En este sentido, algunos autores denominan este derecho como de autodeterminación informativa y se trata de poder conocer y controlar la gestión de la información personal, esto es, qué información existe, quién tiene acceso a ella, quién tiene capacidad para crear y difundir información sobre terceras personas, para qué se usan estos datos personales, qué decisiones se toman con ellos, etc.

Para ampliar información puede consultar los siguientes textos:

- Constitución Española. Art. 18.4.
- Tribunal Constitucional, Pleno, Sentencias 254/1993, 290/2000 y 292/2000.

2 ¿A QUIÉN PERTENECEN LOS DATOS?

- **Los datos personales pertenecen a las personas a las que se refieren** y sólo ellas pueden decidir sobre los mismos. **Por tanto, los diferentes servicios o departamentos municipales no son dueños de los datos.**
- Hay leyes que permiten que los servicios o departamentos de una entidad local puedan tener datos de una persona incluso sin su consentimiento.
- Sólo se pueden utilizar respetando la normativa sobre protección de datos de carácter personal.

3 ¿ES APLICABLE LA NORMATIVA DE PROTECCIÓN DE DATOS A LOS DATOS DE LAS PERSONAS FALLECIDAS?

- **Las personas fallecidas no son titulares del derecho** a la protección de datos personales.
- No obstante, los datos de carácter personal referentes a personas fallecidas o el dato del fallecimiento de una persona, **en cuanto sean datos personales relativos a otras personas (sus hijos/as, sus herederos/as, etc.),** pueden ser considerados datos de carácter personal y **sí son objeto de protección,** a efectos de aplicación de la normativa sobre protección de datos.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 2.
- Dictamen AVPD CN06-013.

4 LOS TRÁMITES ADMINISTRATIVOS Y COMUNICACIONES POR VÍA ELECTRÓNICA ¿ESTÁN SUJETOS AL RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES?

- La ley no establece distinciones según el tipo de soporte en que los datos son tratados. Por ello, también **los trámites administrativos que se realicen mediante la administración electrónica quedan sujetos a** los requerimientos que la **normativa sobre protección de datos establece.**
- Los datos personales que se manejan en las tramitaciones administrativas telemáticas integrarán los correspondientes ficheros, que habrán de ser creados y declarados para su inscripción en el Registro de Protección de Datos de Euskadi. Respecto de los mismos, deberá solicitarse el consentimiento, excepto que una ley lo prevea y se deberá informar a la persona afectada.

5 REVELAR DATOS PERSONALES A TRAVÉS DE UNA PÁGINA WEB ¿CONSTITUYE UN TRATAMIENTO DE DATOS PERSONALES?

- Hacer referencia en una página web a una persona e identificarla por su nombre o por otros medios, como su número de teléfono, y facilitar información relativa a sus condiciones de trabajo o a sus aficiones, constituye un tratamiento de datos de carácter personal. Por tanto, es necesario cumplir las previsiones establecidas en la Ley.

- Hemos de ser conscientes de la facilidad con la que se pueden encontrar referencias personales en páginas web mediante el uso de buscadores, especializados en rastrear datos en sitios o documentos a través de internet.

Para ampliar información puede consultar los siguientes textos:

- Tribunal de Justicia de las Comunidades Europeas, Sentencia de 6 de noviembre de 2003. Caso LINDQVIST.

6 ¿QUÉ SON DATOS PERSONALES?

- Se entiende por “dato personal” cualquier información (numérica, alfabética, gráfica, fotográfica, acústica, etc.) relativa a una persona física identificada o identificable.

- El término “identificable” no se aplica cuando se requeriría una gran cantidad de tiempo y de esfuerzo para identificar a una persona a partir de los datos utilizados en varios ficheros o documentos. Tampoco se aplica la normativa sobre protección de datos personales si la información es anónima o si se presenta como datos agregados (por ejemplo, el perfil de la estructura de edad de los trabajadores de una organización).

- Los ficheros municipales suelen incluir datos personales como los siguientes: nombre y apellidos, DNI, teléfono, domicilio, titulaciones académicas y datos formativos, fecha de nacimiento, nacionalidad, sexo, actividades profesionales, demanda de actividades culturales y deportivas, datos bancarios, impuestos, vehículos en propiedad, inmuebles en propiedad, diversas prestaciones sociales, demanda de actividades formativas, ayudas y subvenciones, circunstancias sociales, ingresos y rentas.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 3.

7 ¿QUÉ SON DATOS PERSONALES ESPECIALMENTE PROTEGIDOS?

- Algunos datos tienen la consideración de particularmente delicados, en cuanto a que pertenecen a la esfera más íntima de la persona o a que su comunicación pueden hacerla vulnerable. Por ello, son reconocidos como datos especialmente protegidos, de tal manera que su tratamiento conlleva un plus de medidas para garantizar su seguridad. Estos datos son los que revelan, respecto a una persona, su ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual e infracciones penales o administrativas.

- Respecto a los datos de ideología, religión o creencias, nadie puede ser obligado a declarar.

- Para el tratamiento de datos que revelen la **ideología, afiliación sindical, religión y creencias,** será necesario el consentimiento expreso y por escrito de la persona afectada.

- Y para el tratamiento de datos que hagan referencia al **origen racial, a la salud y a la vida sexual** es imprescindible el consentimiento expreso de la persona.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 7 y 8.

8 ¿QUÉ FICHEROS SUELEN DECLARAR LAS ENTIDADES LOCALES?

- Las entidades locales están obligadas a declarar en el Registro de Protección de Datos de Euskadi todos los ficheros que generan para el ejercicio de sus competencias legales, siempre que incluyan datos personales.

- Los ficheros declarados más comunes son: Padrón Municipal de habitantes, Gestión de tasas y tributos, Registro de entradas y salidas, Gestión contable, Prestación de servicios sociales (asistencia e integración social), Gestión de personal y nómina, Gestión de alumnos de escuelas (infantiles, de música, artísticas, etc.), Socios y usuarios de instalaciones deportivas, Bienes inmuebles propiedad rústica, Animales domésticos, Gestión de cementerio, Urbanismo.

Para ampliar información puede consultar los siguientes textos:

- Consultar Registro de Protección de Datos en www.avpd.es.
- Ley 7/1985, de 2 de abril, reguladora de Bases de Régimen Local. Art. 25.

9 ¿QUÉ SIGNIFICA "TRATAMIENTO DE DATOS", SEA MANUAL O AUTOMÁTICO?

- La expresión "tratamiento de datos" incluye la recogida, conservación, combinación, comunicación o cualquier otra forma de utilización de datos personales, sea de forma manual o informatizada. En ocasiones, un tratamiento de datos es tanto manual como automático, pues es habitual combinar los métodos de archivado tradicionales con sistemas informáticos, de tal manera que éstos últimos conservan sólo una parte de los datos disponibles y remiten a los archivos para el resto de la información.

10 ¿CUÁL ES LA DIFERENCIA ENTRE FICHEROS AUTOMATIZADOS Y FICHEROS MANUALES?

- Un fichero es un conjunto organizado de datos de carácter personal, cualquiera que sea el modo o la forma en la que se ha creado, se almacena, se organiza o por la que se accede.
- De forma progresiva, los ficheros utilizados por los entidades locales se han ido automatizando, esto es, consisten en grupos de información estructurada en bases de datos y necesitan de la informática para su procesamiento, almacenamiento y explotación. Por ello, se les llama también ficheros informáticos.
- No obstante, las entidades locales conservan ficheros o conjuntos organizados de expedientes también en formato papel.
- La normativa de protección de datos personales se aplica tanto a ficheros automatizados como a ficheros manuales. Las medidas que buscan garantizar la seguridad de la información se adecuan al formato, informático o manual, del fichero.

11 ¿SE HAN DE DECLARAR E INSCRIBIR EN EL REGISTRO DE PROTECCIÓN DE DATOS DE EUSKADI LOS FICHEROS MANUALES EN PAPEL, TALES COMO FICHAS, LISTADOS, ETC.?

- Los conjuntos organizados de datos que se tratan en un formato manual (conjuntos de expedientes, listados estructurados, fichas clasificadas u organizadas, etc.) se han de crear y declarar para su inscripción en el Registro de Protección de Datos de Euskadi.

12 ¿QUÉ NORMA O DISPOSICIÓN HAN DE EMPLEAR LAS ENTIDADES LOCALES PARA CREAR LOS FICHEROS DE DATOS PERSONALES?

- La Ley Orgánica 15/1999 establece que los ficheros han de crearse, modificarse o suprimirse por **disposición de carácter general.** Ahora bien, el concepto “disposición de carácter general” no es extrapolable de manera directa al sistema normativo municipal.

- Habitualmente las entidades locales han declarado los ficheros mediante una Ordenanza o un Reglamento y, en menor medida, mediante un Decreto de Alcaldía. En la actualidad, la Agencia Vasca de Protección de Datos (AVPD) admite, como disposición de creación, la Ordenanza, el Reglamento e, incluso, el Decreto de Alcaldía.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 20.
- MBP Entidades Locales. Art.15. Anexo II M6.

13 ¿CÓMO SE PRESENTA LA SOLICITUD DE INSCRIPCIÓN DE FICHEROS EN LA AVPD?

- En la página web de la AVPD (www.avpd.es) se puede obtener un programa de auto declaración e instrucciones para cumplimentar los formularios de inscripción de los ficheros en el Registro de Protección de Datos de Euskadi.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Art.16.
- Decreto 308/2005, de 18 de octubre de desarrollo de la Ley 2/2004. Art.2.
- Resolución de 21 de julio de 2005 del Director de la AVPD por la que se establecen los modelos normalizados.

14 CUANDO SE MODIFICAN O SUPRIMEN FICHEROS DE DATOS PERSONALES DE TITULARIDAD PÚBLICA, ¿CÓMO SE HACE LA DECLARACIÓN DE ESTA MODIFICACIÓN O SUPRESIÓN?

- Los ficheros de las entidades locales se modifican o suprimen mediante una disposición del mismo rango que la que los creó.

- Esta modificación o supresión también ha de ser notificada a la AVPD. En la página web de la AVPD (www.avpd.es) se puede obtener un programa de auto declaración e instrucciones para cumplimentar los formularios para notificar los cambios y solicitar su inscripción en el Registro de Protección de Datos de Euskadi.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Art.16.
- Decreto 308/2005, de 18 de octubre de desarrollo de la Ley 2/2004. Art.2.
- Resolución de 21 de julio de 2005 del Director de la AVPD por la que se establecen los modelos normalizados.

15 EL ALCALDE O LA ALCALDESA HA DECIDIDO REORGANIZAR LAS RESPONSABILIDADES DE LAS DISTINTAS CONCEJALÍAS ¿DEBEN NOTIFICARSE ESTOS CAMBIOS A LA AVPD?

- Si estos cambios internos de responsabilidades entre concejalías suponen modificaciones en cuanto a las personas que asumen responsabilidades sobre ficheros de datos, tal y como constan inscritos en el Registro de Protección de Datos de Euskadi, en estos casos sí es necesaria su notificación a la AVPD.

- Por ejemplo, si el órgano Responsable del Fichero “Usuarios de instalaciones deportivas municipales” era la concejalía de cultura, pero se crea una concejalía de deportes que asume tales funciones, este cambio debe ser comunicado a la AVPD, para su inscripción. Además, se ha de remitir una copia de la norma municipal que regula el cambio en las responsabilidades.

16 ¿CÓMO TIENE QUE DECLARAR SUS FICHEROS UNA MANCOMUNIDAD DE MUNICIPIOS?

- Las mancomunidades de municipios de la Comunidad Autónoma del País Vasco han de declarar sus ficheros ante la Agencia de Protección de Datos de Euskadi, a través de la elaboración de una ordenanza, o un acuerdo del organismo rector o una disposición de carácter general en la forma prevista en la legislación básica de Régimen Local y en sus Estatutos.

17 ¿CÓMO TIENE QUE DECLARAR SUS FICHEROS UN CONSORCIO?

- Los consorcios en los que participen municipios de la Comunidad Autónoma del País Vasco han de declarar sus ficheros ante la Agencia de Protección de datos de Euskadi, a través de la elaboración de una ordenanza o disposición de carácter general en la forma prevista en la legislación básica de Régimen Local y en sus Estatutos.

18 ¿CÓMO TIENEN QUE DECLARAR SUS FICHEROS LAS CUADRILLAS DEL TERRITORIO HISTÓRICO DE ÁLAVA?

- Las cuadrillas del Territorio Histórico de Álava han de declarar sus ficheros ante la Agencia de Protección de datos de Euskadi, a través de la elaboración de una ordenanza o disposición de carácter general en la forma prevista en la legislación específica y en su propio Reglamento de Funcionamiento.

Para ampliar información puede consultar los siguientes textos:

- Norma Foral 63/1989, de 20 de noviembre, de Cuadrillas.

19 ¿CÓMO TIENEN QUE DECLARAR SUS FICHEROS LOS CONCEJOS DEL TERRITORIO HISTÓRICO DE ÁLAVA?

- Los concejos del Territorio Histórico de Álava han de declarar sus ficheros ante la Agencia de Protección de datos de Euskadi, a través de la elaboración de una ordenanza o reglamento en la forma prevista en la legislación básica de Régimen Local y en la Norma Foral 11/1995, de 20 de marzo, de Concejos del Territorio Histórico de Álava.

Para ampliar información puede consultar los siguientes textos:

- Norma Foral 11/1995, de 20 de marzo, de Concejos del Territorio Histórico de Álava.

20 ¿ES NECESARIO DECLARAR LOS FICHEROS EN LA AGENCIA VASCA DE PROTECCIÓN DE DATOS (AVPD) Y TAMBIÉN EN LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD)?

- No es necesario declarar los ficheros de las entidades locales en ambos registros, el de la AVPD y el de la AEPD. El acto de notificación a la AVPD se considerará también notificación a la AEPD y la AVPD se encarga de trasladar la información a aquella.
- Existe un protocolo de colaboración entre las cuatro agencias existentes en el Estado (española, madrileña, catalana y vasca) por el que se establece un sistema de intercambio registral.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Art. 16.

21 ¿DÓNDE HAN DE DECLARARSE LOS FICHEROS DE EMPRESAS MUNICIPALES?

- Los ficheros de empresas municipales deberán declararse ante la Agencia Española de Protección de Datos (AEPD).

Para ampliar información puede consultar los siguientes textos:

- Ley 2/2004, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos. Art. 2.

22 ¿CONOCE LA AVPD LOS DATOS PERSONALES RECOGIDOS EN LOS FICHEROS DECLARADOS ANTE ELLA?

- El Registro de Protección de Datos de Euskadi, que gestiona la AVPD, no contiene datos personales, sino sólo información sobre las características de los ficheros de las entidades locales.
- En concreto, la información que contiene el Registro de Protección de Datos de Euskadi es:
  - Tipo de administración.
  - Responsable del Fichero.

- Dirección postal para acceder al fichero.
- Nombre del fichero.
- Descripción del fichero.
- Disposición general en la que se publicó.
- Nivel de seguridad aplicable.
- Cesiones de los datos.
- Descripción de la finalidad.
- Procedencia de datos.
- Procedimiento de recogida.
- Soporte (papel, automatizado, otros).
- Estructura de datos.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Arts. 15 y 16.
- Consultar Registro en la página www.avpd.es.

23 ¿QUIÉNES PUEDEN SER RESPONSABLES DE FICHEROS EN LAS ENTIDADES LOCALES?

- La figura del Responsable del fichero o tratamiento es una persona, física o jurídica, de naturaleza pública o privada, o un órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento de los datos personales.

- En una entidad local, es su Presidencia la responsable de todos los ficheros o, alternativamente, cualquier órgano de la misma cuando así esté previsto en su estructura orgánica.

- La Presidencia podrá delegar en una persona física, de entre su personal, la realización de tareas operativas relacionadas con la seguridad de los ficheros. Normalmente las delegaciones se producen a favor de personas que ocupan puestos de concejal, secretario o secretaria, director o directora, etc.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Arts. 25 3 b).

24 ¿QUÉ AGENTES ACTIVOS SUELEN INTERVENIR EN PROTECCIÓN DE DATOS EN UNA ENTIDAD LOCAL?

- Atendiendo a la estructura de cada entidad local, se identifican las siguientes figuras, como posibles agentes en la protección de datos de carácter personal en cada organización:
  - **a)** La persona que presida la entidad local asumirá la máxima responsabilidad.
  - **b)** La persona Responsable de Fichero: puede ser la misma persona que ocupa la alcaldía u otra persona en quien delegue.
  - **c)** Responsable de Seguridad.
  - **d)** Los usuarios y usuarias (personas o procesos autorizados a acceder a datos o recursos).
  - **e)** Persona o entidad Encargada del tratamiento (persona física o jurídica que trata datos personales por cuenta del Responsable del fichero).
  - **f)** Una Comisión para la protección de datos personales.
  - **g)** Persona colaboradora o coordinadora en materia de protección de datos.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Arts. 25 3 b).

25 ¿QUÉ SE ENTIENDE POR CONSENTIMIENTO?

- Se entiende por consentimiento toda manifestación de voluntad mediante la cual la persona interesada consiente el tratamiento de los datos personales que la conciernen.

- Esta manifestación de voluntad o consentimiento ha de ser:
  - Libre, esto es, un consentimiento no prestado por error, violencia, intimidación o dolor.
  - Inequívoca (no presunta).
  - Específica, esto es, referida a una determinada operación de tratamiento y para una finalidad explícita.
  - Informada, es decir, que la persona conoce, de forma previa al tratamiento, la existencia de éste y sus finalidades.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Arts. 3 y 6.

26 ¿CUÁNDO Y EN QUÉ FORMA SE SOLICITA EL CONSENTIMIENTO?

- Cuando se van a recoger datos de carácter personal que después se tratarán en ficheros, se ha de solicitar el consentimiento del titular de los datos, esto es, de la persona a la que los datos se refieren.

- El consentimiento siempre tiene que ser **inequívoco**, esto es, no presunto, lo quiere decir que debe existir expresamente una acción u omisión que implique la existencia del consentimiento.

- El consentimiento puede ser:
  - **Tácito:** se informa, se solicita el consentimiento y comunica que se entenderá otorgado si no hay una manifestación en contra.
  - **Expreso:** se informa, se solicita y debe otorgarse expresamente de manera verbal.
  - **Expreso y por escrito:** se informa, se solicita y debe otorgarse expresamente de manera escrita (este procedimiento es obligatorio con datos relativos a ideología, religión, creencias y afiliación sindical).

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Arts. 6 y 7.
- MBP Entidades Locales. Arts. 20 y 21.

27 ¿CUÁNDO NO ES NECESARIO SOLICITAR EL CONSENTIMIENTO?

- No será necesario solicitar el consentimiento cuando:
  - Existe una ley que autoriza el tratamiento de los datos.
  - Los datos se necesitan para el ejercicio de competencias de las entidades locales.
  - En un contrato o precontrato entre el entidad local y una persona (titular de datos personales) existe una relación laboral, negocial o administrativa y los datos son necesarios para el mantenimiento o cumplimiento de la relación.
  - Está en juego la vida de una persona.
  - Los datos personales se recogen de fuentes accesibles al público, si se cumplen otras condiciones.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Arts. 6 y 7.
- MBP Entidades Locales. Arts. 20 y 21.
- Ley 7/1985, de 2 de abril, reguladora de Bases de Régimen Local Art. 25.

28 ¿QUÉ ES EL DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS? ¿DE QUÉ SE HA DE INFORMAR?

- Las personas a las que se soliciten datos personales deben ser previamente informadas de manera expresa de:
  - Que existe un fichero o tratamiento de datos personales.
  - Su finalidad y de los destinatarios de la información.
  - Si es obligatorio o no responder a las preguntas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
  - De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
  - Y de la identidad y dirección del responsable del tratamiento de datos.

- La cuestión esencial es la siguiente: ¿pueden las personas comprender las implicaciones de la información que tienen que dar a la administración? Los individuos deben disponer de información suficiente para tomar decisiones y poder dar su consentimiento (consentimiento informado).

29 SI A UNA PERSONA SE LE SOLICITAN DATOS DE FORMA VERBAL ¿DE QUÉ MANERA SE LE INFORMA DE LO QUE LE ATAÑE (DERECHO DE INFORMACIÓN)?

- La información se ha de proporcionar a través de un medio que sea coherente con el sistema de recogida de los datos.
- La información que se ha de facilitar es la misma aunque se comunique verbalmente, por escrito o por vía electrónica.
- Cuando se recogen datos de forma verbal también será necesario informar de modo expreso, preciso e inequívoco:
  - **Expreso:** bien verbalmente, bien por escrito mediante la entrega de una nota informativa.
  - **Preciso:** dando la información necesaria sobre todos los aspectos descritos en la pregunta nº 27, sobre qué es el derecho a la información (fichero, finalidad, destinatarios, dirección del responsable, carácter de su respuesta, derechos acceso, etc.).
  - **Inequívoco:** evitando datos o detalles que hagan la información inadecuada, inexacta o que induzca al error.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 5.
- MBP Entidades Locales. Art. 6.

30 SI A UNA PERSONA SE LE SOLICITAN DATOS PERSONALES MEDIANTE UN FORMULARIO ESCRITO, ¿DE QUÉ MANERA SE LE INFORMA DE LO QUE LE ATAÑE (DERECHO DE INFORMACIÓN)?

- Si se recogen datos personales mediante cuestionarios o impresos escritos debe figurar claramente en los mismos la siguiente información:
  - La existencia de un fichero, la finalidad de la recogida de éste y los destinatarios de la información.
  - La identidad y dirección de la persona responsable del tratamiento.
  - El carácter obligatorio o facultativo de su respuesta.
  - Las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
  - La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

- Si el diseño del documento conlleva el uso de un tamaño de letra sensiblemente reducido para las cláusulas informativas, se complementará la información a suministrar a través de carteles instalados en un lugar visible y destacado en las oficinas de atención ciudadana. De manera similar, la información puede publicarse en la página web de la entidad local.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 5.
- MBP Entidades Locales. Art. 6 y Anexo M1.1.

31 SI A UNA PERSONA SE LE SOLICITAN DATOS PERSONALES MEDIANTE LA PÁGINA WEB, ¿DE QUÉ MANERA SE LE INFORMA DE LO QUE LE ATAÑE (DERECHO DE INFORMACIÓN)?

- Normalmente se utilizarán cuestionarios o impresos adaptados a la página web. En los mismos deben figurar con claridad las cláusulas informativas, que son las mismas que las de los impresos no electrónicos o que las verbales:
  - La existencia de un fichero, de la finalidad de la recogida de éste y de los destinatarios de la información.
  - La identidad y dirección de la persona responsable del tratamiento.
  - El carácter obligatorio o facultativo de su respuesta.
  - Las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
  - La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

- Si, excepcionalmente, el diseño del documento impide o desaconseja la inclusión de las cláusulas informativas, se complementará la información a suministrar a través de un enlace dentro de la misma página web, donde se ofrecerá dicha información.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 5.
- MBP Entidades Locales. Art. 6 y Anexo M1.1.

32 ¿DEBE DARSE UNA INFORMACIÓN DIFERENTE EN LA RECOGIDA DE DATOS ESPECIALMENTE PROTEGIDOS?

- En la recogida de datos especialmente protegidos en conveniente dar la información por escrito. Será necesario informar de modo:
  - **Expreso:** por escrito mediante la entrega de una nota informativa.
  - **Preciso:** dando la información necesaria:
    - De la existencia de un fichero, de la finalidad de la recogida de éste y de los destinatarios de la información.
    - De la identidad y dirección de la persona responsable del tratamiento.
    - Del carácter obligatorio o facultativo de su respuesta.
    - De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
    - De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
  - **Inequívoco:** evitando datos o detalles que hagan la información inadecuada, inexacta o que induzca a error.

- Adicionalmente, es necesario advertir:
  - Si son datos de ideología, religión y creencias, que nadie está obligado a declarar.
  - Si son datos de ideología, religión, creencias y afiliación sindical, en que el consentimiento deberá ser expreso y por escrito.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 5.
- MBP Entidades Locales. Art. 6 y Anexo M1.1.

33 ¿QUÉ SE ENTIENDE POR “CALIDAD DE LOS DATOS”?

- Es uno de los principios básicos de la protección de datos y garantiza a las personas que sus datos serán:
  - Recogidos por medios lícitos, leales y no fraudulentos.
  - Tratados para propósitos explícitos y limitados y no para otros fines distintos.
  - Adecuados, pertinentes y no excesivos.
  - Exactos y puestos al día.
  - No almacenados más tiempo que el necesario.

34 ¿QUÉ SON DATOS ADECUADOS, PERTINENTES Y NO EXCESIVOS?

- Los datos son **adecuados** cuando sen los más apropiados para responder a las circunstancias y condiciones de la finalidad que se pretende con la recogida de información.
- Los datos son **pertinentes** si tienen relación y conciernen o conducen a la finalidad que se pretende con la recogida de información.
- Los datos serán **no excesivos** si no van más allá de lo lícito y razonable para conseguir la finalidad que se pretende con la recogida de información.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 4.
- MBP Entidades Locales. Art. 18.

35 ¿QUÉ SE ENTIENDE POR FINALIDADES DETERMINADAS, EXPLÍCITAS Y LEGÍTIMAS?

- Son **finalidades determinadas** aquéllas que están claramente **concretadas, que son precisas, que no son vagas.**
- Son **finalidades explícitas,** las que **expresan claramente y de manera determinada** una cosa.
- Son **finalidades legítimas** aquellas que son **conformes a las leyes.**

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 5.
- MBP Entidades Locales. Art. 18.

36 ¿QUÉ ES UN ENCARGADO O ENCARGADA DE TRATAMIENTO?

- Es una persona, empresa, autoridad pública, servicio o cualquier otro organismo que trata datos personales por cuenta de la administración o de la persona Responsable de Fichero. Por ejemplo, respecto de algunos tratamientos de los Ayuntamientos de Gipuzkoa es IZFE.

- En la medida en la que tratan datos personales han de establecer y cumplir todas las medidas de seguridad que resulten de aplicación.

- El nuevo Reglamento de 2007, que desarrolla la LOPD, redefine el concepto de encargado de tratamiento, de tal manera que también pueden serlo órganos administrativos de la propia administración pública, que mantienen con ésta una relación jurídica. Asimismo, entes sin personalidad jurídica, como las uniones temporales de empresas (UTE), pueden actuar también como encargados de tratamiento cuando actúen como sujetos diferenciados.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Arts. 3 y 12.
- Real Decreto 1720/2007,por el que se aprueba el Reglamento de desarrollo de la de la LOPD. Arts. 20 al 22.
- MBP Entidades Locales. Arts. 5 y 23.

37 ¿CUÁLES SON LOS SUPUESTOS MÁS FRECUENTES DE ENCARGOS DE TRATAMIENTO CON ACCESO A DATOS PERSONALES POR PARTE DE LOS AYUNTAMIENTOS?

- Contratos con empresas para:
  - Realización y mantenimiento de aplicativos informáticos con tratamiento de datos personales (por ejemplo: desarrollo de aplicación de gestión de tributos, de gestión de impuestos, etc.)
  - Gestión de lectura de contadores de agua.
  - Gestión del cobro de determinadas tasas o impuestos.
  - Gestión de la seguridad y salud laboral.
  - Gestión de envío de documentación (con empresas de mailing).
  - Gestión del pago de la nómina o de la coordinación del pago de impuestos (entidades financieras).
  - Seguridad física de instalaciones.

- Gestión de la destrucción de papeles y listados.
- Limpieza.
- Elaboración de la nómina por asesorías externas.
- Entidades financieras para coordinar el pago de nómina.

38 ¿QUÉ CLÁUSULAS, RELACIONADAS CON LA PROTECCIÓN DE DATOS, TIENEN QUE INCLUIRSE EN EL CONTRATO CON UNA ENTIDAD SI ÉSTA VA A ACCEDER A FICHEROS MUNICIPALES CON DATOS PERSONALES?

- El ayuntamiento ha de **regular la realización del tratamiento de datos personales por parte de la entidad contratada,** a quién se reconocerá como encargada de tratamiento. Esta regulación se ha de realizar preferentemente mediante un contrato escrito, o en cualquier otra forma, siempre que permita acreditar su celebración y contenido.

- El contenido del contrato a firmar incluirá: qué datos se facilitan, en qué fichero está contemplado su tratamiento, para qué tipo de actividad se concreta el trabajo y cómo deben tratarse los datos.

- Las **Obligaciones del encargado de tratamiento** son:
  - Cumplir lo dispuesto en la Ley Orgánica 15/1999.
  - Utilizar la información exclusivamente para la finalidad definida.
  - Tratar la información conforme a las instrucciones.
  - Guardar el secreto profesional tanto la empresa como el personal a su cargo.
  - Cumplir las medidas de seguridad.
  - Poseer un documento de seguridad formalizado y documentado.
  - Informar a la entidad local contratante sobre fallos o fugas del sistema de seguridad.
  - No reproducir, ni comunicar, ni ceder a terceros la información.
  - No subcontratar la actividad, salvo autorización.
  - Borrar los datos o devolver el soporte informático una vez finalizado el servicio contratado.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Arts. 3 y 12.
- MBP Entidades Locales. Arts. 5, 23 y Anexos II M11 y M12.

39 ¿QUÉ DOCUMENTACIÓN ESPECÍFICA ES EXIGIBLE EN LOS "CONTRATOS MENORES" QUE INCLUYAN EN SU OBJETO EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL?

- La formalización de un contrato menor puede realizarse simplemente a través de una factura, comprobante o recibo.

- No obstante, cuando se utilice para tramitar la contratación de bienes o servicios que impliquen el tratamiento de datos personales por parte del contratista, debe existir un documento contractual, elaborado con anterioridad a la realización del servicio contratado, que desarrolle las obligaciones establecidas en el artículo 12 de la Ley Orgánica de Protección de Datos de Carácter Personal y el sometimiento a ellas por el contratista.

- El contenido del contrato incluirá: qué datos se facilitan, en qué fichero está contemplado su tratamiento, para qué tipo de actividad se concreta el trabajo y cómo deben tratarse los datos.

- Las **Obligaciones del encargado de tratamiento** son:
  - Cumplir lo dispuesto en la Ley Orgánica 15/1999.
  - Utilizar la información exclusivamente para la finalidad definida.
  - Tratar la información conforme a las instrucciones.
  - Guardar el secreto profesional tanto la empresa como el personal a su cargo.
  - Cumplir las medidas de seguridad.
  - Poseer un documento de seguridad formalizado y documentado.
  - Informar a la entidad local contratante sobre fallos o fugas del sistema de seguridad.
  - No reproducir, ni comunicar, ni ceder a terceros la información.
  - No subcontratar la actividad, salvo autorización.
  - Borrar los datos o devolver el soporte informático una vez finalizado el servicio contratado.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Arts. 3 y 12.
- MBP Entidades Locales. Arts. 5, 23 y Anexos II M11 y M12.

40 ¿QUÉ ES UNA FINALIDAD INCOMPATIBLE RESPECTO A AQUELLA PARA LA CUAL FUERON SOLICITADOS LOS DATOS?

- Los datos de carácter personal no pueden utilizarse para finalidades incompatibles con aquéllas para las que los datos fueron recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.
- Son **finalidades incompatibles** aquéllas que no pueden unirse o concurrir con la inicialmente prevista.
- Existe jurisprudencia que establece que los datos personales recogidos para una finalidad concreta no pueden ser utilizados para cualquier otra finalidad distinta, aunque fuera compatible con la que originó la recogida de los datos. Para poder hacerlo habría que solicitar el consentimiento de la persona afectada.
- Por ejemplo, no pueden utilizarse los datos personales del fichero municipal sobre impuesto de circulación, cuya finalidad es el cobro del impuesto, para asignar tarjetas personalizadas de aparcamientos de residentes, sin pedir antes el consentimiento. Sin embargo, si respecto a los datos del fichero de impuesto de circulación, se utilizan técnicas de disociación para con los datos personales y se transforma la información en datos agregados, se podrán utilizar estos datos generales para planificar el reparto de tarjetas OTA, porque ya no se están tratando datos personales.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 4.
- MBP Entidades Locales. Art. 18.

41 EN LA GESTIÓN DE INFORMACIÓN PERSONAL ¿QUÉ SE ENTIENDE POR DATOS PERSONALES EXACTOS Y PUESTOS AL DÍA?

- Los datos de carácter personal han de ser exactos y puestos al día, de manera que respondan con veracidad a la situación actual del afectado.
- Son **datos exactos** aquellos que responden con fidelidad y ajustadamente a la situación del afectado.
- Son **datos puestos al día** los datos que están actualizados, es decir, que responden a la situación real del afectado en cada momento.

- Las entidades locales han de realizar operaciones periódicas para posibilitar la actualización y exactitud de la información que manejan. Esto implica que en ocasiones tendrán que preguntar a los propios ciudadanos si los datos personales que la entidad local tiene de ellos son exactos y actualizados o, por el contrario, han cambiado.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 4.
- MBP Entidades Locales. Art. 18.

42 ¿QUÉ ES UN DOCUMENTO DE SEGURIDAD?

- El documento de seguridad es un documento aprobado por la persona Responsable del Fichero y recoge las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente.
- Es de obligado cumplimiento para el personal con acceso a los sistemas de información y tiene carácter de documento interno de la organización.
- A estos efectos, se entiende por sistemas de información el conjunto de ficheros automatizados y manuales, programas informáticos, soportes y equipos empleados para el almacenamiento y tratamiento de los datos de carácter personal.
- Los documentos de seguridad están entendidos como unidad en la que se incluyen estándares, normas, impresos, contratos, manifestaciones de voluntad, decálogos, códigos de conducta y rutinas, todo ello sometido no sólo a la normativa de protección de datos, si no a toda norma que concurra con el tratamiento de información referida a personas físicas identificadas o identificables.
- El documento de seguridad puede ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o para un grupo de ficheros o tratamientos.

43 ¿QUÉ ESTRUCTURA DEBE TENER UN DOCUMENTO DE SEGURIDAD?

- El documento deberá contener, como mínimo, los siguientes aspectos:
  - Ámbito de aplicación del documento y los recursos protegidos.
  - Medidas de seguridad (normas, procedimientos, reglas y estándares) para garantizar el nivel de seguridad exigido en la normativa vigente y en este Manual de Buenas Prácticas.
  - Funciones y normas de conducta obligatoria común para el personal que trata datos personales.
  - Estructura de los ficheros con datos personales y descripción de los sistemas de información que los tratan.
  - Procedimiento de notificación, gestión y respuesta ante las incidencias.
  - Los procedimientos de realización de copias de respaldo y de recuperación de los datos en ficheros automatizados.

- Medidas a adoptar para el transporte de soportes y documentos.
- Medidas a adoptar cuando un soporte tenga que ser desechado o reutilizado.
- Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento de seguridad.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Anexo IV D1. Esquema Documento de Seguridad.

44 ¿QUÉ ES UN REGISTRO DE INCIDENCIAS?

- Una **incidencia** es cualquier evento que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad de la información, entendida en sus tres vertientes de confidencialidad, integridad y disponibilidad de los datos.
- Así, sucesos como el olvido de contraseñas, la pérdida de archivos, entradas de virus o las revisiones de mantenimiento de los equipos informáticos deben considerarse como incidencias.
- El **registro de incidencias** garantiza la prevención y la seguridad de la información y es una herramienta imprescindible para la elaboración de los informes periódicos de autocontrol. Normalmente es una base de datos o programa informático específico que permite notificar y gestionar todas las incidencias.
- De cada incidencia deberá registrarse la siguiente información: el tipo de incidencia, fecha y hora en que se ha producido, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

45 ¿CUÁLES SON LAS INCIDENCIAS MÁS FRECUENTES?

- Las incidencias más habituales son:
  - Olvido de clave de usuario y contraseña.
  - Solicitud de acceso a determinados recursos de red (discos, impresoras, aplicaciones, etc).
  - Recuperación de archivos desde copias de seguridad.

46 ¿QUÉ SON UNA RELACIÓN DE USUARIOS, LOS PERFILES DE USUARIO Y LOS ACCESOS AUTORIZADOS?

- Una **relación de usuarios** es una relación de personas autorizadas a acceder a un sistema de información.
- Los **perfiles de usuario** son los accesos autorizados para un grupo de usuarios.
- Los **accesos autorizados** son autorizaciones concedidas a una persona usuaria para la utilización de los diversos recursos, entendidos como cualquier parte componente de un sistema de información.
- Los usuarios tienen acceso solamente a aquellos recursos que necesitan para desarrollar sus funciones.
- Es el responsable de fichero quien se encarga de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

47 ¿QUÉ SON LAS CONTRASEÑAS DE ACCESO? ¿QUÉ ES UN PROCEDIMIENTO DE GESTIÓN DE CONTRASEÑAS?

- Se denomina contraseña a la **llave virtual** que utiliza un usuario de una red o de un sistema informático para entrar en la red o en el sistema informático.
- La contraseña o llave de acceso del usuario se compone de dos partes: el identificador y el código de autenticación.
- El **identificador o nombre de usuario** tiene dos funciones: identificar o reconocer al usuario autorizado y definir la capacidad de obrar del usuario dentro del sistema. Es personal, intransferible y secreto.
- El **código de autenticación** permite la comprobación de la identidad de una persona usuaria, representa su firma y, al igual que su nombre de usuario, es personal, intransferible y secreto.
- Un **procedimiento de gestión de contraseñas** es una herramienta que nos permite atender tanto las incidencias relacionadas con contraseñas ocurridas a los usuarios como el funcionamiento ordinario de altas y bajas de nuevos usuarios.

- Por ejemplo, establece cuáles son los pasos a seguir cuando hay que dar de alta un usuario nuevo: quién tiene que autorizarlo, cómo se comunica la autorización, a qué aplicaciones concretas o partes de la aplicación y en qué condiciones puede acceder, etc.

48 ¿CUÁLES SON LAS RECOMENDACIONES ESTÁNDAR RESPECTO AL USO DE CONTRASEÑAS?

- Longitud mínima de 6 caracteres; recomendado 8; no más de 16.
- Utilizar tanto mayúsculas como minúsculas, incluyendo algunos números y signos de puntuación.
- Cambiar la contraseña periódicamente (por ejemplo, cada tres meses), sin seguir un ciclo para ellas.
- Coloquialmente: *"Una contraseña debe ser como un cepillo de dientes: Úsalo cada día, cámbialo regularmente, y NO lo compartas con tus amigos"*.

49 ¿QUÉ ES LO QUE NO HAY QUE HACER CON LAS CONTRASEÑAS?

- No utilizar nombres, topónimos, etc., ni palabras que puedan figurar en un diccionario de cualquier idioma.
- No utilizar datos personales o familiares evidentes, como DNI´s, teléfonos, matrículas de coche, e-mail, fechas significativas, etc.
- No utilizar una única contraseña para todos los servicios, cuentas, bancos, etc.
- No compartir la contraseña, ni apuntarla en un papel ni en un fichero de texto, ni enviarla por correo electrónico, SMS, mensajería instantánea, etc., ni mucho menos colocarla en un post-it en la pantalla del ordenador.
- No facilitar la contraseña por teléfono por correo, ni verbalmente a un compañero de trabajo.
- Las contraseñas largas y complicadas, que se han de cambiar a menudo, se terminan apuntando en algún lugar no muy lejano del teclado.

50 RECOMENDACIONES PARA HACER MÁS FÁCIL LA GESTIÓN DE CONTRASEÑAS

- Todos tenemos muchas contraseñas, debemos cambiarlas con cierta frecuencia y debemos recordarlas o recuperarlas en cualquier momento o lugar. Los siguientes consejos pretenden ilustrar diferentes maneras de combinar fortaleza de la contraseña con facilidad para gestionar y recordar.

1. Tener tres contraseñas base: la buena, la fea y la mala

- Elegir un conjunto de tres contraseñas base para poder utilizarlas en servicios y accesos con diferentes requerimientos de seguridad:
- La “mala”, para utilizar en pruebas, usos temporales, servicios y accesos poco importantes, que podáis, llegado el caso, comunicar a otros sin peligro real. No necesita reunir todos los requerimientos de seguridad, basta con que sea sencilla de recordar. (ejemplo: cacatua).
- La “buena”, para todos los demás servicios o accesos, con todos los requisitos de seguridad. Recomendable que tenga justamente ocho caracteres, pues algunos servicios tienen esa limitación. (ejemplo: KaKa-tu4).
- La “fea”, para aquellos servicios de seguridad reforzada, como puede ser un PUK, una segunda clave de confirmación, programas de gestión de contraseñas, etc. Impronunciable, pero recordable. (ejemplo: #K4.K/\-7u+@#).

2. Utilizar una ristra de pines

- Elegir como base una ristra de 16 números, y para recordarlos mejor, dividirlos en cuatro grupos de cuatro. Una vez memorizados, nos proporcionaran muchos grupos de números: cada grupo de cuatro, los primeros (o segundos, o..) de cada grupo, cada grupo en orden inverso, etc. Nos servirán tanto para los servicios con pines numéricos como para combinar con otras contraseñas.
- No usar DNI´s, teléfonos, matrículas de coches, aniversarios, etc.

3. Frases de paso, en vez de palabras de paso

- Escoger una frase aleatoria de un libro, o un poema, o la letra de una canción (ojo con las evidentes), y escoger las primeras letras de cada palabra. La frase puede ser en otro idioma (“En un lugar de La Mancha” = euldLM).

4. Recordar una regla, en vez de cien contraseñas

- Cuando se tienen muchas contraseñas, a partir de las contraseñas base, se pueden generar varias series de contraseñas, mediante reglas propias de transformación. Estas reglas son, precisamente, las que han de ser personales y las que les darán fortaleza a las familias de contraseñas que así se construyan. Por ejemplo: si se combinan contraseñas y ristras, para recordar se puede apuntar en papel o fichero, haciendo referencia a cómo aplicar la regla, no al resultado: ("la buena, más el segundo grupo").

5. Guardar las contraseñas con una contraseña

- Cuando no se recurre a una regla de combinación, y por lo tanto nos encontramos con muchas contraseñas, lo ideal es utilizar un fichero cifrado o un programa de gestión de contraseñas, que las guarda internamente de forma cifrada (para estos casos utilizaríamos la contraseña "fea").

51 ¿QUÉ SOPORTES SE UTILIZAN PARA ALMACENAR O TRASLADAR LA INFORMACIÓN?

- Distinguimos dos clases de soportes:
  - **Soportes analógicos:** son los medios más tradicionales de almacenamiento: el papel, cintas videocasete, cintas de radiocasete, etc.
  - **Soportes digitales:** nos permiten una capacidad de almacenamiento mucho mayor y también mayor capacidad de proceso. Podemos incluir desde los ya poco usados discos flexibles o disquetes hasta los diferentes dispositivos de memoria no volátil como memorias USB o diferentes tarjetas de memoria, pasando por las cintas magnéticas, discos duros o todo tipo de discos ópticos (CD, DVD y los nuevos llegados a este grupo como HD-DVD o Blue – Ray).

52 ¿QUÉ OPERACIONES SE DEBEN REALIZAR PARA ELIMINAR DEFINITIVAMENTE LOS DATOS PERSONALES CONTENIDOS EN UN SOPORTE CUANDO SE DEJA DE UTILIZAR?

- Cuando se quiere inutilizar un soporte tenemos que tomar las medidas adecuadas para que no se puedan recuperar los datos del mismo, teniendo en cuenta el tipo de soporte: tal vez tengamos que utilizar una **destructora de papel o formatear un disquete.**

- Uno de los casos más frecuentes es qué hacemos con el ordenador viejo cuando procedemos a la actualización de un puesto de trabajo. En estos casos, nos debemos asegurar de que una vez que está pasada toda la información del ordenador viejo al nuevo, **se destruye (no se borra)** con alguna utilidad existente y creada al efecto, **toda la información del ordenador viejo para hacerla irrecuperable.**

- Actualmente uno de los soportes más utilizados para el traslado de información son las **memorias USB**, por lo que debemos ser cautelosos con la información que trasladamos en las mismas. Además de borrar la información, hemos de asegurarnos de que no se pueda recuperar **(el simple borrado no es suficiente, pues existen programas de recuperación).** Puede ser necesario el apoyo o el asesoramiento de técnicos especializados.

53 ¿QUÉ SON COPIAS DE SEGURIDAD, DE RESPALDO O DE RECUPERACIÓN?

- Una **copia de seguridad o copia de respaldo** (backup en inglés) se refiere a la copia de información, de tal forma que estas copias adicionales puedan restaurar un sistema después de una pérdida de información.

- La copia de seguridad es útil por varias razones:
  - Para restaurar un ordenador a un estado operacional previo, después de un desastre **(copias de seguridad del sistema).**
  - Para restaurar un pequeño número de ficheros después de que hayan sido borrados o dañados accidentalmente **(copias de seguridad de datos).**
  - En el supuesto de copias de seguridad de ficheros con datos personales, las mismas son una garantía de que, ante un accidente o pérdida de información, no tengamos que acudir a solicitar de nuevo toda la información perdida a los ciudadanos.

54 ¿A QUIÉN SE DEBE DESIGNAR COMO RESPONSABLE DE SEGURIDAD DE UN FICHERO?

- El Responsable de Seguridad de un fichero es la persona encargada de coordinar y controlar las medidas técnicas, lógicas y organizativas definidas en el Documento de Seguridad.
- Por tanto, ha de ser una persona con las atribuciones o el respaldo suficientes dentro de la organización para poder realizar, u ordenar la realización, de cualquier acción o procedimiento que así venga definido en el Documento de Seguridad.
- Está obligada a realizar una auditoría interna periódica y a dar cuenta del grado de cumplimiento de las medidas de seguridad exigidas por el documento de seguridad o reglamento interno de seguridad.

Para ampliar información puede consultar los siguientes textos:

- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Art. 95.

55 ¿EN QUÉ CONSISTE UN AUDITORÍA SOBRE LAS MEDIDAS DE SEGURIDAD?

- Podemos definir una Auditoría como un proceso sistemático, independiente y documentado para obtener evidencias de análisis y evaluarlas de manera objetiva, con el fin de determinar el alcance con el que se cumplen el conjunto de políticas, procedimientos o requisitos de seguridad establecidos en el Documento de Seguridad.
- Se consideran evidencias de la auditoría a todo tipo de información verificable y registrada, de un modo u otro.
- Los informes de auditoría son analizados por el Responsable de Seguridad que eleva las conclusiones y propone al Responsable del Fichero las medidas correctoras adecuadas a adoptar.

Para ampliar información puede consultar los siguientes textos:

- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Art. 96.

56 ¿CUÁNDO ES RECOMENDABLE UNA AUDITORÍA INTERNA?

- La auditoría interna es una función asesora que se realiza con recursos humanos y materiales pertenecientes a la propia organización. El auditor, aunque esté vinculado con la organización, debe ser independiente orgánicamente y no haber estado vinculado anteriormente con el sector auditado.
- Habitualmente la auditoría interna se realiza por una decisión de la Dirección con el objeto de emitir informes orientados fundamentalmente a la mejora de la propia organización.

57 ¿CUÁNDO ES RECOMENDABLE UNA AUDITORÍA EXTERNA?

- La auditoría externa es un examen crítico realizado por una firma especializada en auditoría. El encargo de este examen puede ser por iniciativa de la Dirección, pero normalmente se deriva del cumplimiento de obligaciones o compromisos formales y, además, el objeto del informe de auditoría suele ser la presentación del mismo a un tercero.
- La firma auditora no debe mantener ninguna otra relación con la firma auditada, ni haber participado de ninguna manera en el ciclo de vida de ninguno de los objetos de la auditoría.

58 ¿CÓMO SE CIFRAN LOS DATOS?

- “Codificar o cifrar” es transformar un conjunto de datos legibles en un conjunto de datos ilegibles o, al menos, ininteligibles. El proceso inverso se denomina “descodificar o descifrar”.
- Existen diferentes programas que permiten automatizar las tareas de codificado y descodificado y que exigen mayor o menor labor de computación, en función de la complejidad del sistema de cifrado.
- Los **sistemas de cifrado** se llaman **"sistemas criptográficos" y pueden codificar textos escritos y también la voz**. Las personas que inventan los sistemas de cifrado reciben el nombre de criptógrafas; a su vez, los criptoanalistas son las personas que se dedican al desciframiento de estos sistemas.

59 ¿CUÁLES SON LAS MEDIDAS ORDINARIAS DE PROTECCIÓN DE FICHEROS DE DATOS MANUALES?

- Los ficheros manuales se clasifican, al igual que los ficheros automatizados, en virtud del carácter de la información personal de la que son objeto. Así, se clasifican en niveles básico, medio y alto según las medidas de seguridad que les resulten de aplicación De esta manera, las cautelas que debemos cumplir en cada caso, en cuanto al acceso, la custodia, etc., son equiparables a las de los ficheros automatizados de su correspondiente nivel de seguridad, siempre teniendo en cuenta sus diferente carácter.

- Entre las diferentes medidas se pueden citar: utilización de armarios en zonas con control de accesos, cierres con llaves, elementos de seguridad que eviten que se puedan destruir (detectores), inventarios, acceso limitado a personas autorizadas, etc.

Para ampliar información puede consultar los siguientes textos:

- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Capítulo IV del Título VIII.
- MBP Entidades Locales. Anexo IV D5. Cuadro de Niveles de Seguridad.

60 ¿CÓMO SE DEBE ACTUAR CUANDO SEA NECESARIO SOLICITAR EL CONSENTIMIENTO PARA LAS CESIONES DE DATOS?

- Los datos de carácter personal sólo podrán ser comunicados a una tercera persona o entidad cuando se cumplan las siguientes condiciones:
  - La cesión se realiza para cumplir fines directamente relacionados con las funciones legítimas de la entidad local y de la parte a la que se ceden.
  - La cesión se realiza con el **previo consentimiento** de las personas titulares de los datos, con las excepciones establecidas en la ley.

- El **procedimiento para ceder datos** es el siguiente:
  - Solicitud de cesión de datos.
  - Carta de condiciones a aceptar por la entidad solicitante.
  - Solicitud del consentimiento previo de las personas titulares de datos, excepto cuando no sea necesario.
  - Cesión de los datos.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 11.
- MBP Entidades Locales. Arts. 42, 43 y Anexo II M15.

61 ¿EN QUÉ SITUACIONES NO ES NECESARIO SOLICITAR EL CONSENTIMIENTO PARA LAS CESIONES DE DATOS?

- No será necesario solicitar el consentimiento en las cesiones de datos:
  - 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.
  - Cuando la comunicación sea al Defensor del Pueblo, al Ararteko, al Ministerio Fiscal o a los Jueces o Tribunales o al Tribunal de Cuentas y al Tribunal Vasco de Cuentas Públicas, en el ejercicio de las funciones que tienen atribuidas.
  - Cuando la cesión se produzca entre administraciones públicas con fines históricos, estadísticos o científicos.
  - Cuando la cesión de datos personales relativos a la salud sea necesaria para solucionar una urgencia o para realizar estudios epidemiológicos.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 11.
- MBP Entidades Locales. Art. 42.

62 ¿CUÁNDO Y EN QUÉ CONDICIONES SE PUEDEN SOLICITAR CESIONES DE DATOS A OTRAS ADMINISTRACIONES?

- Si una entidad local necesita datos de carácter personal podrá solicitarlos a otras administraciones (otras entidades locales, departamentos de las diputaciones forales, departamentos del Gobierno Vasco, etc.):
  - Cuando tenga constancia de que aquella administración posee los datos que necesita.
  - Cuando tenga la competencia para realizar la actividad para la cual se requiere el fichero con los datos personales solicitados. Debe acreditar esta competencia.
- Una vez realizada la solicitud, la administración a la que se le ha solicitado la cesión determinará: si es un supuesto en el que se requiere consentimiento expreso de las personas titulares de los datos o si la cesión está amparada en alguna de las situaciones previstas en el artículo 11 de la Ley Orgánica 15/1999.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 11.
- MBP Entidades Locales. Art. 45.

63 ¿CUÁNDO Y EN QUÉ CONDICIONES SE PUEDEN CEDER DATOS A OTRAS ADMINISTRACIONES?

- Si una entidad local es requerida por otras administraciones (entidades locales, departamentos de las diputaciones forales, departamentos del Gobierno Vasco, etc.) para la cesión de datos, ha de seguir el protocolo oportuno, en función de que sea necesario o no el consentimiento de las personas titulares de los datos:

- Cuando para la cesión sea necesario el consentimiento, el procedimiento es el siguiente:
  - Solicitud de cesión de datos personales.
  - Carta de condiciones a aceptar por la entidad que solicita los datos.
  - Solicitud del consentimiento a las personas titulares de datos.
  - Cesión de los datos personales.
- Cuando para la cesión no sea necesario el consentimiento, el procedimiento es el siguiente:
  - Solicitud de cesión de datos personales.
  - Carta de condiciones a aceptar por la entidad que solicita los datos.
  - Cesión de los datos personales.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 11.
- MBP Entidades Locales. Art. 44.

64 ¿EN QUÉ CONDICIONES SE PUEDEN SOLICITAR Y CEDER DATOS A OTROS DEPARTAMENTOS Y SERVICIOS EN EL SENO DE LA PROPIA ENTIDAD LOCAL?

- Para la tramitación de un expediente administrativo no es admisible el uso compartido de un fichero en el que se incluyen datos personales. Tampoco es admisible compartir el fichero con otro órgano de la propia entidad local para el desarrollo de una competencia de ésta, si esta función no está expresamente contemplada entre las finalidades del fichero de datos.

- Hay una excepción a esta imposibilidad: la cesión de datos del Padrón Municipal de Habitantes para el ejercicio de una competencia que corresponde a la propia entidad local, respecto a la cual el domicilio es un dato relevante. En este supuesto, no será necesario el consentimiento de la persona interesada pues se entiende que existe compatibilidad de fines.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 11.
- MBP Entidades Locales. Arts. 45 al 4.

65 ¿ES ADECUADO QUE LOS CENTROS EDUCATIVOS DEL MUNICIPIO, PÚBLICOS O PRIVADOS, PIDAN DATOS DEL DOMICILIO DE LOS NIÑOS NACIDOS EN UN DETERMINADO AÑO PARA HACER UNA CAMPAÑA PROMOCIONAL DE MATRICULACIÓN?

- La cesión de datos del Padrón a una ikastola o centro educativo privado sin consentimiento previo de los titulares de los datos, o sus representantes si son menores, no se ajusta la normativa en materia de protección de datos.
- La cesión de datos del Padrón a un centro educativo público debería cumplir el requisito de que tales datos sean necesarios para el ejercicio de las respectivas competencias de ambas administraciones y exclusivamente para asuntos en los que el domicilio sea un dato relevante. Es dudoso que un centro público tenga la competencia relativa a la promoción de la matriculación educativa, pues ésta parece estar en manos del Departamento de Educación del Gobierno Vasco, a través de sus servicios centrales o territoriales.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 11.
- MBP Entidades Locales. Art. 45-4.
- AVPD Dictamen CN006-08.

66 ¿ES ADECUADO QUE LOS DEPARTAMENTOS DEL GOBIERNO VASCO PIDAN DATOS PERSONALES A LOS AYUNTAMIENTOS PARA REALIZAR CAMPAÑAS DE COMUNICACIÓN ESPECÍFICAS? ¿EXISTEN OTRAS ALTERNATIVAS PARA HACERLO?

- Frecuentemente los departamentos del Gobierno Vasco plantean peticiones de información a los ayuntamientos justificando que los datos del censo de éstos son los más actualizados. Por ejemplo, el Departamento de Sanidad solicita periódicamente datos para realizar la campaña de prevención del cáncer de mama.
- Como norma general, la cesión de datos del Padrón a otra administración deberá cumplir el requisito de que tales datos sean necesarios para el ejercicio de las competencias de ambas administraciones y que se utilicen exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes.

- Existe una alternativa, a tenor de lo establecido en 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, en su Disposición Adicional Segunda. En esta ley se articula que el EUSTAT - Instituto Vasco de Estadística puede facilitar a las diferentes administraciones de la CAPV los datos personales que le soliciten, a partir de la copia de los datos actualizados del fichero de Padrón que recibe periódicamente de los ayuntamientos. Las administraciones solicitantes han de acreditar que tienen la competencia para realizar la actividad que pretenden y que el domicilio es un dato relevante para la misma.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 11.
- MBP Entidades Locales. Art. 45.
- AVPD Dictamen CN06-018.
- Ley 2/2004, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos. Disposición Adicional Segunda.

67 ¿PUEDEN CEDERSE DATOS DEL PADRÓN MUNICIPAL A PERSONAS FÍSICAS O EMPRESAS PRIVADAS?

- Es frecuente que empresas de nueva instalación en un municipio soliciten al ayuntamiento correspondiente el Padrón de habitantes con el fin de enviar publicidad sobre sus productos a los residentes.

- Sin embargo, está cesión no es posible porque el uso de los datos del Padrón municipal está restringido a la finalidad que la ley le confiere.

- Para estas actividades de publicidad comercial, las empresas privadas o personas físicas pueden dirigirse a empresas de marketing directo que sí pueden disponer de bases de datos personales para usos publicitarios.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 11.
- MBP Entidades Locales. Art. 45.

68 ¿CUÁL ES EL PROCEDIMIENTO PARA CANCELAR DATOS PERSONALES?

- Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permitan la identificación de las personas titulares de los datos durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

- Los datos se cancelarán destruyéndolos físicamente o, en su caso, mediante técnicas de disociación que no permitan la identificación de las personas titulares de los mismos.

- Si están en un fichero automatizado se borrarán de tal manera que no sea posible su recuperación. No es suficiente el borrado físico ordinario, sino que es necesario un borrado "especializado" realizado por técnicos informáticos o por otro personal al que se le hayan transmitido las instrucciones técnicas precisas.

- Si los datos están en soporte papel se destruirán mediante destructoras de papel o a través de empresas especializadas que se comprometan a hacerlo de una forma segura.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 4.

69 ¿CUÁL ES EL PROCEDIMIENTO PARA BLOQUEAR DATOS SIN CANCELARLOS?

- En ocasiones los datos han dejado de ser necesarios para la finalidad para la cual fueron recabados o registrados, pero es necesario mantenerlos por requerimientos legales o contractuales, esto es, porque existe un procedimiento judicial en marcha, para satisfacer necesidades de conocimiento histórico, estadístico o científico o para atender posibles responsabilidades nacidas del tratamiento. En estos casos, los datos son sometidos a un procedimiento de bloqueo.

- El bloqueo es la identificación y reserva de un dato o grupo de datos personales, que imposibilita su tratamiento y permite el acceso sólo cuando se da alguna de las situaciones descritas.

- Transcurrido el plazo de prescripción de dichas situaciones especiales, el dato bloqueado se cancela.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 4.

70 ¿CÓMO SE HAN DE DESTRUIR LOS DATOS PERSONALES QUE SE ENCUENTRAN EN SOPORTE PAPEL (LISTADOS, EXPEDIENTES, ETC.)?

- Los datos de carácter personal son cancelados cuando ya no son necesarios o pertinentes para la finalidad para la cual han sido recabados o registrados.
- Se cancelan destruyéndolos físicamente o sometiéndolos a una técnica de disociación que no permita la identificación de la persona titular del dato personal.
- Si los datos personales están en soporte papel se destruirán mediante destructoras de papel o a través de empresas especializadas que se comprometan a hacerlo de una forma segura.
- Para aplicar la técnica de disociación a los datos personales que se encuentran en soporte papel será necesario destruir las referencias que permitan la identificación de la persona titular de los datos. La disociación puede realizarse mediante un procedimiento de borrado o pintado que no permita su visionado o recuperado mediante ninguna técnica.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 4.

71 ¿CÓMO FACILITAR A LOS CIUDADANOS EL EJERCICIO DE SUS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN RESPECTO AL TRATAMIENTO DE SUS DATOS PERSONALES?

- Las entidades locales han de facilitar a las personas el ejercicio de los derechos de acceso, rectificación, cancelación y oposición**,** conocidos como derechos ARCO. Para ello, tienen que realizar las siguientes acciones:
  - Rediseñar los procedimientos administrativos, si es necesario, para que el ejercicio de los derechos ARCO (acceder a datos, rectificarlos, etc.) no resulte una tarea complicada para la administración ni para el ciudadano.
  - Diseñar modelos de documentos, en formato papel, electrónico, etc., para que, mediante su cumplimentación, se facilite el ejercicio de derechos ARCO. A estos efectos podrán utilizar los modelos que se acompañan en el presente Manual.
  - Dar una formación adecuada a los empleados públicos con funciones de Atención a la Ciudadanía, para que informen a los ciudadanos de los derechos que tienen y les orienten para que puedan ejercerlos.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Art. 22, Anexos III P1.1 y P1.2 y Anexos II M2, M3, M4 y M5.

72 ¿QUÉ ES EL DERECHO DE ACCESO Y CÓMO SE SOLICITA?

- Es el derecho que tiene cualquier persona a preguntar y obtener de su entidad local información de qué datos de carácter personal tiene acerca de ella, del detalle de los mismos, de las finalidades para los que se almacenaron, de la procedencia de los datos y de las comunicaciones o cesiones de datos realizadas o que se prevén efectuar.

- **Cómo solicitar acceso a los datos personales propios:**
  - Solicitarlo la persona interesada o su representante legal.
  - Dirigir la solicitud a la persona designada como responsable del fichero.
  - Se puede solicitar una vez cada 12 meses, como norma general.
  - El ejercicio del derecho de acceso es gratuito.
  - Plazo para responder afirmativa o negativamente a la petición de acceso: 30 días. Si es afirmativa, se ha de facilitar el acceso en los próximos 10 días desde la estimación positiva del derecho.

- **Procedimiento de tutela del derecho.** Si la persona solicitante entiende que no se le ha facilitado correctamente el derecho de acceso a sus propios datos (no se le ha contestado en 30 días, la contestación ha sido negativa, etc.) puede reclamar ante la Agencia Vasca de Protección de Datos.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 15.
- Ley 2/2004, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vascs de Protección de Datos. Art. 8.
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Arts. 27 y 30.
- MBP Entidades Locales. Art. 7, Anexo II M2.

73 ¿ES POSIBLE DENEGAR EL EJERCICIO DEL DERECHO DE ACCESO POR LA DIFICULTAD O EL ELEVADO COSTE QUE PUEDE SUPONER SU EJERCICIO?

- No. En este sentido, la LOPD prevé que los datos de carácter personal sean almacenados de forma que permitan el ejercicio del derecho de acceso.
- Además, el acceso a los datos es gratuito.
- No obstante, este derecho será ejercitado en intervalos de tiempo iguales o superiores a doce meses, salvo que la persona interesada acredite un interés legítimo, en cuyo caso podrá ejercitarlo en un período de tiempo inferior al estipulado.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 15.
- Ley 2/2004, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos. Art. 8.
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Arts. 27 y 30.
- MBP Entidades Locales. Art. 7, Anexo II M2.

74 ¿QUÉ ES EL DERECHO DE RECTIFICACIÓN Y CÓMO SE SOLICITA?

- Es el derecho que tiene cualquier persona a solicitar de una entidad local que rectifique, corrija o complete datos suyos si son inexactos, inadecuados, incompletos o excesivos.

- **Cómo solicitar la rectificación de los datos personales propios:**
  - Solicitarlo la persona interesada o su representante legal.
  - Dirigir la solicitud a la persona designada responsable del fichero.
  - Indicar a qué datos se refiere y la corrección que haya de realizarse y acompañarla de la documentación justificativa de lo solicitado.
  - El ejercicio del derecho de rectificación es gratuito.
  - El responsable del fichero resolverá y, en su caso, rectificará los datos, en el plazo máximo de 10 días desde la recepción de la solicitud.

- **Procedimiento de tutela de sus derechos.** Si el solicitante entiende que no se le ha facilitado correctamente el derecho de rectificación de sus propios datos, no se le ha contestado en 10 días o la contestación ha sido negativa, puede reclamar ante la Agencia Vasca de Protección de Datos.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 16.
- Ley 2/2004, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos. Art. 8.
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Arts 31 y 33.
- MBP Entidades Locales. Art. 8, Anexo II M3.

75 ¿QUÉ ES EL DERECHO DE CANCELACIÓN Y CÓMO SE SOLICITA?

- Es el derecho de cualquier persona a solicitar de una entidad local que cancele datos suyos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la que se obtuvieron o se haya superado el período necesario para el cumplimiento de los fines para los que fueron recabados.

- **Cómo solicitar la cancelación de los datos personales propios:**
  - Solicitarlo directamente la persona interesada o su representante legal.
  - Dirigir la solicitud a la persona designada responsable del fichero.
  - El ejercicio del derecho de cancelación es gratuito.
  - El responsable del fichero resolverá, y en su caso cancelará los datos, en el plazo máximo de 10 días desde la recepción de la solicitud.

- La cancelación implica el borrado físico de los datos personales, excepto cuando la cancelación no sea materialmente posible; en este caso, el responsable del fichero bloqueará los datos con el fin de impedir su tratamiento.

- **Procedimiento de tutela del derecho.** Si el solicitante entiende que no se le ha facilitado correctamente el derecho de cancelación de sus propios datos, no se le ha contestado en 10 días o la contestación ha sido negativa, puede reclamar ante la Agencia Vasca de Protección de Datos.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 16.
- Ley 2/2004, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos. Art. 8.
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Art. 31 y 33.
- MBP Entidades Locales. Art. 9, Anexo II M4.

76 ¿EN QUÉ CIRCUNSTANCIAS NO SE PUEDEN CANCELAR LOS DATOS PERSONALES?

- No se pueden cancelar los datos personales cuándo tales datos personales deban ser conservados durante determinados plazos temporales.

- Estos períodos de tiempo durante los cuales los datos no pueden ser cancelados se establecen según las disposiciones legales que sean de aplicación o se derivan, en su caso, de los contratos o de las relaciones contractuales existentes entre el responsable de tratamiento (persona o entidad) y la persona interesada, contratos que han sido el origen del tratamiento de los datos personales en cuestión.

- En estos supuestos, transcurrido el plazo de conservación de los datos personales, se han de bloquear éstos, estando a disposición exclusivamente de las administraciones públicas, jueces y tribunales para atender las posibles responsabilidades surgidas del tratamiento y durante el plazo de prescripción de éstas. Cuando finaliza este plazo los datos personales han de suprimirse. (VER SUPUESTO 68)

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 16.
- Ley 2/2004, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos. Art. 8.
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Arts. 31 y 33.
- MBP Entidades Locales. Art. 9.

77 ¿QUÉ ES EL DERECHO DE OPOSICIÓN Y CÓMO SE SOLICITA?

- Es el derecho de cualquier persona a solicitar de una entidad local que no realice el tratamiento de sus datos personales o que cese en el mismo en los siguientes supuestos:

  a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario. (…)

  b) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida a la persona afectada y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

- **Cómo solicitar la oposición de los datos personales propios:**
  - Solicitarlo directamente la persona interesada o su representante legal.
  - Dirigir la solicitud a la persona designada responsable del fichero.
  - El ejercicio del derecho de oposición es gratuito.
  - El responsable del fichero resolverá, y en su caso excluirá del tratamiento los datos relativos a la persona solicitante, en el plazo máximo de 10 días desde la recepción de la solicitud. Si deniega la solicitud de oposición, deberá hacerlo motivadamente, también en el plazo de 10 días. En el caso de que no disponga de datos de carácter personal del solicitante, deberá igualmente comunicárselo en el mismo plazo.

- **Procedimiento de tutela de sus derechos.** Si el solicitante entiende que no se le ha facilitado correctamente el derecho de oposición, no se le ha contestado en 10 días o la contestación ha sido negativa, puede reclamar ante la Agencia Vasca de Protección de Datos.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Arts. 6,4 y 17.
- Ley 2/2004, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos. Art. 8.
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Art. 95. Arts. 34 y 36.
- MBP Entidades Locales. Art. 9, Anexo II M5.

78 ¿QUÉ SE ENTIENDE POR DECISIONES QUE AFECTAN SIGNIFICATIVAMENTE A LOS CIUDADANOS Y QUE ESTÁN BASADAS ÚNICAMENTE EN UN TRATAMIENTO AUTOMATIZADO DE DATOS?

- Las personas tienen derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas, o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta. **Los ciudadanos podrán ejercer el derecho de oposición respecto de estas decisiones.**

- No obstante, los afectados podrán verse sometidos a una de las decisiones arriba mencionadas cuando se hayan adoptado en el marco de un contrato celebrado a petición del interesado, siempre que se le dé la posibilidad de alegar lo que estime pertinente. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas arriba y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

- También podrán verse sometidos a alguna decisión como las descritas arriba cuando esté autorizada por una ley que establezca medidas que garanticen el interés legítimo de la persona interesada.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art.13.
- MBP Entidades Locales. Art. 12
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Art.36.

79 SI LOS DERECHOS DE UNA PERSONA CON RELACIÓN A SUS DATOS PERSONALES, NO SON ATENDIDOS ¿CÓMO SE PUEDE SOLICITAR LA TUTELA DE LA AVPD?

- El ciudadano tiene derecho a reclamar ante la AVPD, para que ésta inicie un procedimiento de tutela de derechos, cuando le haya sido denegado, total o parcialmente, el ejercicio de los derechos de Acceso, Rectificación, Cancelación, u Oposición, o cuando crea que no se le ha facilitado o atendido el ejercicio de esos derechos.

- En la página web de la AVPD (www.avpd.es), en el apartado ciudadanos, se encuentran disponibles unos modelos de formularios para solicitar el inicio del procedimiento de tutela y la relación de documentos que es necesario aportar.

- El plazo máximo para dictar y notificar una resolución de tutela de derechos es de 6 meses.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art.18.
- Ley 2/2004, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos. Art. 9.
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Arts 30.3 y 33.3.
- MBP Entidades Locales. Art. 14.

80 ¿CÓMO SE PUEDE CONSULTAR EL REGISTRO DE PROTECCIÓN DE DATOS DE EUSKADI?

- Los ciudadanos tienen derecho a consultar en el Registro de Protección de Datos de Euskadi la información sobre la existencia de tratamientos de carácter personal realizados por una entidad local, sus finalidades y la identidad del responsable del fichero.

- La consulta se podrá realizar de diversas formas: solicitando la consulta por escrito, a través de correo electrónico o accediendo directamente a la función consulta del Registro, dentro de la página web www.avdp.es.

- La consulta a través de la página web www.avdp.es. permite distintas posibilidades de selección y de búsqueda, así como la generación de la información en ficheros en formato pdf., que se podrán imprimir o descargar en el ordenador propio.

- El Registro no contiene información de datos personales concretos, sino de características de los ficheros declarados, de los tipos de datos que contienen y de los tipos de tratamientos que se realizan con ellos.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art.14.

81 ¿CÓMO PUEDE UNA PERSONA EVITAR QUE LE LLEGUE PUBLICIDAD NO DESEADA?

- Los ciudadanos tienen derecho a conocer de dónde se han obtenido los datos personales propios que se han utilizado para fines de publicidad y prospección comercial. En muchas ocasiones, el origen de sus datos proviene de un consentimiento que se prestó al realizar otra actividad (por ejemplo, cuando se firmó el contrato de uso de una tarjeta de fidelización).

- Se puede revocar en cualquier momento el consentimiento en virtud del cual se recibe la publicidad.

- En todo momento es factible oponerse a este tratamiento de datos personales, sin necesidad de justificarlo, mediante petición expresa y sin coste alguno, y solicitar la cancelación de los datos personales, que serán dados de baja de forma inmediata. Se puede ejercer el derecho a oponerse ante el comerciante (responsable de tratamiento). El procedimiento ha de ser sencillo: un teléfono gratuito, un mensaje de correo electrónico o a través de un servicio de quejas o de atención al cliente.

- Asimismo la Federación Española de Comercio Electrónico y Marketing Directo (FECEMD) coordina un registro, denominado Lista Robinson, en el que se puede inscribir cualquier persona que no quiera recibir publicidad directa de ninguna empresa con la que no tenga una relación comercial.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art.30.
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Arts. 45 al 51.

82 ¿QUÉ PUEDE HACER UNA PERSONA PARA NO FIGURAR EN GUÍAS TELEFÓNICAS?

- Las personas tienen derecho a conocer de dónde se han obtenido los datos personales propios que han sido utilizados en una guía telefónica.

- Además, podrán oponerse a este tratamiento de datos personales, sin necesidad de justificarlo, mediante petición expresa de cancelación de sus datos en la lista, dirigida a la empresa editora de la guía o a la persona o entidad que figure como responsable del fichero. Este derecho de oposición es gratuito y los datos personales serán dados de baja de forma inmediata y no serán considerados para futuras ediciones.

- Un modelo de formulario para ejercer el derecho de oposición puede consultarse en la página web de la AVPD (www.avpd.es).

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art.30.
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Arts. 45 al 51.

ANEXO I

SUPUESTOS CONCRETOS

2. GESTIONES ESPECÍFICAS DENTRO DE LOS AYUNTAMIENTOS

83 ¿SE DEBE CREAR EL FICHERO DEL PADRÓN MUNICIPAL DE HABITANTES? ¿SE DEBE INSCRIBIR EN EL REGISTRO DE DATOS PERSONALES DE EUSKADI?

- El Padrón Municipal es un registro administrativo donde constan los vecinos de un municipio.
- El Padrón Municipal es también un fichero con datos personales que existe en todas las entidades locales. Sus finalidades son:
  - Determinar la población del municipio
  - Constituir prueba de residencia en el municipio y del domicilio habitual en el mismo
  - Elaborar estadísticas sobre composición de familias, características económicas, nivel educativo, matrimonio, fecundidad y defunciones.
- El Padrón Municipal debe de crearse y declararse ante la AVPD para que sea inscrito en el Registro de Protección de Datos de Euskadi.

Para ampliar información puede consultar los siguientes textos:

- Ley 7/1985, Reguladora de Bases de Régimen Local. Art. 16.
- MBP Entidades Locales. Art. 45.1.

84 ¿CUÁL ES EL CONTENIDO OBLIGATORIO DEL PADRÓN MUNICIPAL?

- Los datos obligatorios del Padrón son los siguientes:
  - Nombre y apellidos.
  - Sexo.
  - Domicilio habitual.
  - Nacionalidad.
  - Lugar y fecha de nacimiento.
  - Número de documento nacional de identidad o, en el caso de extranjeros, el número de la tarjeta de residencia en vigor.
  - Certificado o título escolar o académico que se posea.
  - Cuantos otros datos puedan ser necesarios para la elaboración del Censo Electoral, siempre que se garantice el respeto a los derechos fundamentales reconocidos en la Constitución.

Para ampliar información puede consultar los siguientes textos:

- Ley 7/1985, Reguladora de Bases de Régimen Local. Art. 16.

85 ¿EN QUÉ CONDICIONES SE PUEDEN CEDER DATOS DEL PADRÓN MUNICIPAL A OTRAS ADMINISTRACIONES?

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

- La administración peticionaria en la solicitud dirigida a la entidad local ha de:
  - Justificar la función que se propone realizar con los datos padronales.
  - Encuadrar dicha función en alguna de las competencias que le reconoce el ordenamiento jurídico, indicándola expresamente en su petición.
  - Acreditar la relevancia de la información de la residencia o el domicilio para la función que quiere llevar a cabo.

Para ampliar información puede consultar los siguientes textos:

- Ley 7/1985, Reguladora de Bases de Régimen Local. Art. 16.
- MBP Entidades Locales. Art. 45.2.

86 ¿EN QUÉ CONDICIONES SE PUEDEN CEDER DATOS DEL PADRÓN MUNICIPAL DENTRO DE LA PROPIA ENTIDAD LOCAL?

- Los datos del Padrón Municipal se cederán a otros servicios o departamentos de la misma entidad local que lo soliciten, sin consentimiento previo de las personas afectadas, solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Art. 45.4.

87 ¿SE PUEDEN CEDER DATOS DEL PADRÓN MUNICIPAL A PERSONAS FÍSICAS O EMPRESAS PRIVADAS?

- No se puede enviar información sobre el Padrón Municipal a personas físicas o empresas privadas.
- Ahora bien, es frecuente que empresas de nueva instalación en el municipio soliciten el Padrón de habitantes al ayuntamiento, con el fin de enviar publicidad a los residentes sobre sus productos. La respuesta a esta petición ha de ser negativa, ya que no es una finalidad que esté reconocida entre las finalidades del Padrón Municipal.

88 ¿SE PUEDEN CEDER DATOS DEL PADRÓN DE UNA ENTIDAD LOCAL A ALGUNA DE SUS JUNTAS ADMINISTRATIVAS PARA REALIZAR PADRONES CONCEJILES? (SÓLO EN EL CASO DE ENTIDADES LOCALES DEL TERRITORIO HISTÓRICO DE ÁLAVA)

- Sí, los datos del Padrón de Habitantes correspondientes a los vecinos de un Concejo podrán ser cedidos por el ayuntamiento que corresponda al Concejo para el fin de crear un padrón concejil.

Para ampliar información puede consultar los siguientes textos:

- Dictamen AVPD CN06-012.

89 ¿SE PUEDE CONTRATAR LA GESTIÓN DEL FICHERO DEL PADRÓN MUNICIPAL CON UNA EMPRESA PRIVADA?

- La formación, mantenimiento, revisión y custodia del Padrón Municipal corresponde a la entidad local que, además, tiene la obligación de gestionarlo por medios informáticos.
- En el supuesto de que las entidades locales no dispongan de una capacidad económica o estructura suficiente para la gestión informática del Padrón Municipal, ésta será realizada por la Diputación Foral que corresponda.

Para ampliar información puede consultar los siguientes textos:

- Ley 7/1985, Reguladora de Bases de Régimen Local. Art. 17.1.

90 ¿QUIÉN TIENE DERECHO AL ACCESO A LA INFORMACIÓN DE EXPEDIENTES MUNICIPALES TERMINADOS? ¿EN QUÉ CONDICIONES SE HA DE FACILITAR ESTE ACCESO?

- Toda persona tiene derecho a obtener una copia de los documentos contenidos en los expedientes terminados, sin que deba exigirse que concurra en la misma persona la condición de interesada directa.
- No obstante, los proyectos técnicos y la documentación compresiva de los mismos, presentados para la obtención de las correspondientes licencias, han de entenderse amparados por el derecho a la propiedad intelectual. Por ello, no se facilitará copia de dicha documentación a una tercera persona, sin autorización expresa de su propietaria.
- El acceso genérico de las personas a la documentación administrativa contenida en los expedientes terminados tiene su límite en el respeto a la intimidad de las personas y en la protección de datos de carácter personal.
- En consecuencia, cuando deba facilitarse documentación que contenga datos de carácter personal, se procurará que dicha información se presente de forma disociada, esto es, eliminando la conexión entre el dato y la persona, despersonalizando el dato y protegiendo la privacidad de la persona.
- Si no fuera posible aplicar un procedimiento de disociación a la información, se procederá a asegurar la ilegibilidad de los datos de carácter personal que contenga la documentación a suministrar, mediante su borrado o tachado.

Para ampliar información puede consultar los siguientes textos:

- Ley 30/1992, de Régimen Jurídico de las AAPP y del Procedimiento Administrativo Común. Arts 35 h. y 37.
- Ley 7/1985, Reguladora de Bases de Régimen Local. Arts. 69 y 70.3.
- MBP Entidades Locales. Art. 48.2.

91 ¿QUIÉN TIENE DERECHO AL ACCESO A LA INFORMACIÓN DE EXPEDIENTES MUNICIPALES EN TRAMITACIÓN? ¿EN QUÉ CONDICIONES SE HA DE FACILITAR ESTE ACCESO?

- El acceso a los documentos que obran 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.

- En los casos en los que se aplique la técnica del silencio administrativo deberá entenderse que, a efectos del ejercicio del derecho de acceso a la información, el procedimiento ha concluido desde la fecha de vencimiento del plazo de resolución y notificación del mismo. Y esto es así con independencia de que, en caso del silencio desestimatorio, la entidad local pueda aún dictar resolución tardía expresa.

Para ampliar información puede consultar los siguientes textos:

- Ley 30/1992, de Régimen Jurídico de las AAPP y del Procedimiento Administrativo Común. Art. 35.a.
- Ley 7/1985, Reguladora de Bases de Régimen Local. Arts. 69 y 70.3.
- MBP Entidades Locales. Art. 48.1.

92 ¿CÓMO ACTUAR ANTE UNA SOLICITUD DE ACCESO A UN DOCUMENTO ADMINISTRATIVO CUYO CONTENIDO O ALCANCE NO PUEDE COMPRENDERSE SIN UNA RELACIÓN O LISTADO DE DATOS PERSONALES? (CON INDEPENDENCIA DE QUE ÉSTA ÚLTIMA FORME PARTE O NO DEL EXPEDIENTE EN EL QUE SE INTEGRA EL DOCUMENTO CUYO ACCESO SE SOLICITA)

- Cuando la solicitud de acceso pueda afectar los derechos e intereses de terceras personas deberá garantizarse la participación en el procedimiento de dichas personas. Para ello, se pondrá en su conocimiento la tramitación del procedimiento de acceso, para que puedan intervenir en él.

- Asimismo, debe contemplarse la posibilidad de facilitar de forma disociada la información contenida en la relación o listado de datos personales, sin que contenga, por tanto, referencias personales. Si esto 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.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Art. 47.7.

93 ¿SE PUEDE FACILITAR INFORMACIÓN SOBRE LAS PERSONAS EMPADRONADAS EN UNA VIVIENDA AL PROPIETARIO DE LA MISMA?

- No es posible facilitar la información de las personas empadronadas en una vivienda ni incluso al propietario de la vivienda.
- No obstante, para poder empadronar en una vivienda a otra persona que no sea su propietaria es necesario que la persona interesada aporte una copia del título o contrato de arrendamiento del piso o una autorización escrita de la persona propietaria (o persona inscrita como principal ocupante de la vivienda) que legitime la ocupación.
- Si bien no es posible facilitar datos personales al propietario de una vivienda que solicita información sobre las personas ocupantes de la misma, sí se puede facilitar información sobre el número de personas ocupantes, sin identificarlas.

Para ampliar información puede consultar los siguientes textos:

- Ley 7/1985, Reguladora de Bases de Régimen Local. Art. 16.1.
- Ley Orgánica15/1999, de Protección de Datos de Carácter Personal. Art. 6 y 11.
- MBP Entidades Locales. Art. 45.
- Real Decreto 2612/1996, Reglamento de Población y Demarcación Territorial de Entidades Locales. Art. 59.2.

94 ¿SE PUEDE FACILITAR UN CERTIFICADO DEL PADRÓN MUNICIPAL DE HABITANTES A UNA PERSONA, DISTINTA DE LA TITULAR DE LOS DATOS PERSONALES, PERO CON QUIEN TIENE UNA RELACIÓN DE PARENTESCO?

- Los datos personales son propiedad de las personas a las que se refieren y sólo ellas, o en el caso de menores o incapacitados sus representantes legales, pueden decidir sobre sus datos personales. En consecuencia, la solicitud de un certificado de empadronamiento debe realizarla la propia persona interesada.
- Ahora bien, se puede arbitrar la posibilidad de que, al tiempo de formular dicha solicitud, la persona titular de los datos manifieste su voluntad o deseo de que otra persona, en su nombre, pueda recoger el certificado de empadronamiento. Esto puede realizarse mediante su mención expresa en la solicitud a través de un espacio específico o un espacio reservado a observaciones.
- Sin esta habilitación expresa no se pueden facilitar certificados con datos personales a personas diferentes de la titular de los datos, sean éstas familiares de la persona o no lo sean.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Art. 17.

95 ¿SE PUEDE FACILITAR UN CERTIFICADO DEL PADRÓN MUNICIPAL DE HABITANTES A UNA PERSONA QUE ES UN FAMILIAR DE OTRA QUE HA FALLECIDO, SI RESULTA NECESARIO PARA LAS GESTIONES RELACIONADAS CON LA HERENCIA Y SEGUROS?

- Sí, se puede facilitar un certificado del Padrón Municipal de Habitantes que contiene datos personales de una persona fallecida a otra persona que es un familiar de la primera. Este hecho no es contrario a la LOPD.

- En principio, las personas fallecidas no son titulares del derecho a la protección de datos personales. No obstante, los datos de carácter personal referentes a personas fallecidas, o el dato del fallecimiento de una persona, en cuanto son datos personales relativos a otras personas (sus hijos o hijas y sus herederos, etc.), pueden ser considerados datos de carácter personal a efectos de aplicación de la normativa sobre protección de datos y sí son objeto de protección.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 2.
- Dictamen AVPD CN06-013.

96 ¿ES ADECUADO PEDIR UN CERTIFICADO TELEFÓNICAMENTE Y ENVIARLO A LA DIRECCIÓN POSTAL DE LA PERSONA TITULAR?

- La realización de consultas y trámites sencillos por teléfono, como la emisión de certificados de empadronamiento, es una funcionalidad concebida como servicio de ayuda a la ciudadanía, en el sentido de que se ofrece a las personas la posibilidad de ahorrar desplazamientos físicos que no son imprescindibles.

- La condición necesaria es la adecuada identificación de la persona que llama por teléfono, a fin de preservar la confidencialidad de la información a suministrar.

- Para solventar esta cuestión se puede identificar a la persona que demanda el servicio solicitándole que nos facilite los datos que nosotros estamos viendo en pantalla. Por ejemplo, si es un volante de empadronamiento lo que nos solicita, pediremos su nombre y DNI, el de su cónyuge, fecha de nacimiento de algún hijo o hija, etc., datos que normalmente sólo puede saber la persona solicitante y, finalmente, remitiremos la documentación siempre a la dirección postal que figura en el Padrón Municipal.

- Otra forma de realizar la identificación de la persona que desea ser atendida por teléfono es mediante el contraste de las claves numéricas (comúnmente conocidas como juego de barcos) que aparece en la tarjeta ONA (Osasun Nortasun Agiria) o tarjeta sanitaria electrónica que procura determinados usos a los ciudadanos.

97 UNA PERSONA QUE RESIDIÓ EN UN AYUNTAMIENTO Y AHORA VIVE FUERA DE ÉL SOLICITA POR TELÉFONO O MEDIANTE INTERNET UN CERTIFICADO DE EMPADRONAMIENTO ¿CÓMO SE DEBE ACTUAR? ¿CÓMO ACREDITAR SU IDENTIDAD?

- La realización de consultas y trámites sencillos por teléfono o a través de internet, como la emisión de certificados de empadronamiento, es una funcionalidad concebida como servicio de ayuda a la ciudadanía, en el sentido de que se ofrece a las personas la posibilidad de ahorrar desplazamientos físicos que no son imprescindibles.
- La condición necesaria es la adecuada identificación de la persona que llama por teléfono, a fin de preservar la confidencialidad de la información a suministrar.
- Para solventar esta cuestión se puede identificar a la persona que demanda el servicio solicitándole que nos facilite los datos que nosotros estamos viendo en pantalla. Por ejemplo, si es un volante de empadronamiento lo que nos solicita, pediremos su nombre y DNI, el de su cónyuge, fecha de nacimiento de algún hijo o hija, etc., datos que normalmente sólo puede saber la persona solicitante y, finalmente, remitiremos la documentación siempre a la dirección postal que figura en el Padrón Municipal.

98 UNA PERSONA SOLICITA UN CERTIFICADO POR CORREO POSTAL, ACREDITA ADECUADAMENTE SU IDENTIDAD (MEDIANTE UN ESCRITO FIRMADO Y CON COPIA DEL DNI) Y PIDE EL ENVÍO DEL CERTIFICADO A UN DOMICILIO AJENO AL QUE CONSTA EN LA INSCRIPCIÓN PADRONAL ¿CÓMO SE DEBE ACTUAR?

- En general, la solicitud de cualquier tipo de certificado ha de formularse por la persona interesada mediante escrito dirigido al ayuntamiento. Podrá realizarse en el impreso normalizado de que disponga la administración municipal en sus oficinas o en el Servicio de Atención Ciudadana, o en un formato electrónico o en cualquier otro formato que libremente elija la persona solicitante.

- En el supuesto planteado, la propia persona interesada, al formalizar la solicitud, ha dado la autorización para este tratamiento concreto de sus datos personales, esto es, para enviarle el certificado padronal a un determinado domicilio. Por tanto, proceder realizar lo solicitado.

Para ampliar información puede consultar los siguientes textos:

- Ley 7/1985, Reguladora de Bases de Régimen Local. Art. 70.
- MBP Entidades Locales. Art.17.

99 CERTIFICADO DE RESIDENCIA Y EMPADRONAMIENTO. PROCEDIMIENTO DE SOLICITUD Y ENTREGA

- El certificado de residencia y empadronamiento acredita la residencia de una persona, mediante la comprobación de su inscripción en el Padrón Municipal de Habitantes del Municipio, ya sea referido al momento actual o de la solicitud ya sea el referido a una fecha anterior (certificado histórico).

- La solicitud de este certificado debe realizarla la persona interesada y, en cuanto a su entrega, puede recogerla otra persona en su nombre si la persona interesada manifiesta esta voluntad.

100 CERTIFICADO HISTÓRICO DE HABITANTE. PROCEDIMIENTO DE SOLICITUD Y ENTREGA

- Se denomina Certificado Histórico de Habitante al certificado de residencia o empadronamiento que acredita la residencia de una persona en un municipio en una fecha anterior al de la emisión del certificado, ya que en el momento actual no se encuentra incluida en el último Padrón Municipal de Habitantes en vigor porque ha causado baja en el mismo.

- El procedimiento de solicitud y entrega es idéntico al del certificado de empadronamiento: la solicitud la realiza la persona interesada y ésta puede manifestar su voluntad de que el certificado sea recogido por otra persona en su nombre.

101 CERTIFICADO DE DEFUNCIÓN. PROCEDIMIENTO DE SOLICITUD Y ENTREGA

- Los certificados de defunción son expedidos por los Registros Civiles; en municipios medianos o pequeños estas funciones se realizan en los Juzgados de Paz.
- El ayuntamiento puede informar a las personas interesadas sobre cómo se realiza este trámite de solicitud del certificado de defunción: qué órgano judicial lo emite, cuáles son los requisitos, etc.
- Si el certificado se solicita por correo ordinario: se remite una carta al Juzgado de Paz en la que se indica el nombre y la dirección postal a la que se quiere que se envíe el certificado; en la solicitud han de constar los siguientes datos:
  - Nombre y apellidos de la persona que solicita el certificado.
  - Si es posible, se detalla el tomo y la página del Libro de Familia en que esté inscrita la defunción.
  - Se indica la clase de certificado, extracto o literal, que se desea.
- Es conveniente incluir un teléfono de contacto para localizar a la persona solicitante en el caso de que sea necesario aclarar algún dato.
- Si el trámite se realiza tras desplazarse al Registro: se debe aportar la documentación siguiente:
  - DNI de la persona que solicite el certificado.
  - Libro de Familia. Si no se aporta, se ha de proporcionar el nombre, apellidos, fecha y lugar de defunción de la persona de la que se solicita el certificado.

102 JUSTIFICANTE DE PAGO. PROCEDIMIENTO DE SOLICITUD Y ENTREGA

- La legislación tributaria determina que las personas que están obligadas a un pago pueden actuar por medio de un representante.
- Por otro lado, cualquier persona puede efectuar el pago y recibir el correspondiente justificante de pago; y esto con independencia de que tenga, o no, interés en el cumplimiento de la obligación, y también independientemente de que la persona obligada al pago sepa de este pago o no o lo apruebe.

- Este pago realizado por una persona distinta a la obligada no supone legitimación para ejercitar ante la administración los derechos que sólo correspondan a la persona obligada al pago.

- En la práctica, suele ser la propia persona interesada, u otra en su nombre, quien realiza el pago material de la deuda tributaria y, acto seguido, se le facilita el documento justificante de la liquidación de la deuda o pago.

Para ampliar información puede consultar los siguientes textos:

- Normativa estatal: Real Decreto 939/2005, por el que se aprueba el ReglamentoGeneral de Recaudación. Arts. 33 y 41.
- Ver normativas Forales: por ejemplo en Bizkaia el Decreto Foral 52/1993, por el que se aprueba el Reglamento de Recaudación del Territorio Histórico de Bizkaia. Arts. 20 y 32.

103 CERTIFICADO DE BIENES. PROCEDIMIENTO DE SOLICITUD Y ENTREGA

- Para acceder a los datos nominativos de los padrones fiscales y obtener documentación de los mismos es necesario disponer del consentimiento, expreso y por escrito, de la persona titular de los datos personales.

- Además del supuesto anterior, se puede acceder a los datos incluidos en un padrón fiscal si los datos personales se encuentran disociados, esto es, se trata de un acceso donde no conste ninguno de los datos protegidos referidos al nombre, apellidos, DNI/CIF y domicilio de quien figura inscrito en los mismos, como titular o sujeto pasivo, así como el valor atribuido de los bienes individualizados.

104 CERTIFICADO DE INCINERACIÓN. PROCEDIMIENTO DE SOLICITUD Y ENTREGA

- Si un familiar de una persona fallecida solicita un certificado de incineración de ésta última, es procedente su emisión y entrega.

- Las personas fallecidas no son titulares del derecho a la protección de datos personales. Ahora bien, los datos de carácter personal que se refieren a personas fallecidas o el dato del fallecimiento de una persona, en la medida en que son datos personales relativos a otras personas -sus hijos e hijas, sus herederos o herederas, etc.-, pueden ser considerados datos de carácter personal a efectos de aplicación de la normativa sobre protección de datos y, en consecuencia, sí son objeto de protección.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 2.
- Dictamen AVPD CN06-013.

105 CERTIFICADO DE CAMBIO DE RESTOS Y TRASLADO DE CENIZAS. PROCEDIMIENTO DE SOLICITUD Y ENTREGA

- Si un familiar de una persona fallecida solicita un certificado de cambio de restos y traslado de cenizas es procedente su emisión y entrega.

- Las personas fallecidas no son titulares del derecho a la protección de datos personales. Ahora bien, los datos de carácter personal que se refieren a personas fallecidas o el dato del fallecimiento de una persona, en la medida en que son datos personales relativos a otras personas -sus hijos e hijas, sus herederos o herederas, etc.-, pueden ser considerados datos de carácter personal a efectos de aplicación de la normativa sobre protección de datos y, en consecuencia, sí son objeto de protección.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 2.
- Dictamen AVPD CN06-013.

106 CERTIFICAR LA BUENA CONDUCTA CIUDADANA. PROCEDIMIENTO DE SOLICITUD Y ENTREGA

- Un ayuntamiento no emite Certificados de Buena Conducta, ya que han sido sustituidos por la Declaración de Conducta Ciudadana, que sobre sí misma ha de formular la propia persona interesada.

- La acreditación de que se carece de antecedentes penales o policiales se realiza mediante la Certificación de Antecedentes Penales, expedida por el Registro Central de Penados y Rebeldes.

- El Ayuntamiento puede informar a la persona que lo solicite sobre cómo realizar la declaración complementaria de conducta ciudadana; ésta ha de incluir los siguientes contenidos:
  - Si la persona que la realiza se encuentra inculpada o procesada.
  - Si se le han aplicado medidas de seguridad o si está implicada en diligencias de seguridad en un procedimiento fundado en la Ley de Peligrosidad Social.
  - Si ha sido condenada en juicios de faltas durante los tres años inmediatamente anteriores a la declaración.
  - Si en los tres años inmediatamente anteriores a la fecha de la declaración, se le ha impuesto sanción gubernativa como consecuencia de expediente administrativo sancionador, por hechos que guarden relación directa con el objeto del expediente en el que se exige la certificación o informe de buena conducta.
  - A tales efectos, no serán objeto de declaración las sanciones gubernativas impuestas por actos meramente imprudentes ni las procedentes de infracciones de tráfico.
  - Si la persona interesada se hallara comprendida en cualquiera de los anteriores supuestos, así lo hará constar, con expresión del órgano jurisdiccional ante el que se hayan seguido las diligencias o que le haya impuesto medidas de seguridad o, en su caso, de la autoridad gubernativa que le hubiere sancionado.

Para ampliar información puede consultar los siguientes textos:

- Ley 69/1980, de Conducta Ciudadana.

107 PUBLICACIÓN DE DATOS PERSONALES EN BOLETINES OFICIALES Y TABLONES DE EDICTOS VIRTUALES ¿QUÉ CAUTELAS DEBEN SEGUIRSE?

- Si la actividad informativa obedece a una decisión discrecional de la entidad local la comunicación que incluya datos de carácter personal sólo puede tener lugar cuando se haya obtenido el consentimiento de las personas interesadas.

- Por el contrario, si la notificación o publicación a través de un boletín oficial o tablón de anuncios responde al cumplimiento de un deber legal fijado con suficiente precisión, nada impide la publicación de datos personales de las personas afectadas. Un supuesto de este tipo es cuando la publicación obedece a propósitos de transparencia, por ejemplo, con ocasión de la publicación de la composición de un Tribunal de Selección, a fin de que la ciudadanía pueda identificar a las personas bajo cuya responsabilidad se va a llevar a cabo un proceso selectivo. Aún cuando la publicación responda a un deber legal, es necesario cumplir los siguientes criterios:
  - Como buena práctica, en la publicación de datos personales en cualquier medio debe acudirse al principio de proporcionalidad. Esto es, sólo se publicarán aquellos datos personales que sean imprescindible para lograr el efecto legal pretendido y que no resulten excesivos.
  - Los boletines oficiales y los tablones de edictos virtuales tienen la consideración de fuentes accesibles al público. En virtud de este carácter, la publicación de datos personales supone facilitar el conocimiento o acceso a terceras personas de datos personales sin el consentimiento de la persona afectada. Por ello, en la publicación oficial debe especificarse que sólo se autoriza el acceso para el fin de dar a conocer su contenido y que no cabe promover un uso abusivo de los datos personales publicados para otras finalidades.

Para ampliar información puede consultar los siguientes textos:

- Ley 30/1992, de Régimen Jurídico de las AAPP y del Procedimiento Administrativo Común. Arts. 60 y 61.
- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art.11.

108 PROCESOS DE CONCURRENCIA COMPETITIVA Y PUBLICACIÓN DE DATOS PERSONALES

- En un procedimiento de concurrencia competitiva la actuación administrativa favorable beneficia sólo a una o algunas de las personas aspirantes, ya que el procedimiento es de naturaleza selectiva y la administración fija los límites. Así, pueden ser procedimientos de concurrencia competitiva la concesión de ayudas económicas o subvenciones, la contratación administrativa de obras, suministros o servicios y los procesos selectivos de personal, entre otros.

- En estos casos, la práctica habitual es publicar la resolución inicial y la final en los boletines oficiales y las comunicaciones de actos de trámite en tablones de anuncios e, incluso, en una página web.

- Aún cuando la publicación responda a un deber legal, es necesario cumplir los siguientes criterios:
  - Como buena práctica, en la publicación de datos personales en cualquier medio debe acudirse al principio de proporcionalidad. Esto es, sólo se publicarán aquellos datos personales que sean imprescindible para lograr el efecto legal pretendido y no resulten excesivos.
  - Cuando se publiquen a través de boletines oficiales o páginas web, como tienen la consideración de fuentes accesibles al público, se facilita el conocimiento o acceso a terceras personas de datos personales sin el consentimiento de la persona afectada. Por ello, en la publicación podrá especificarse que sólo se autoriza el acceso para el fin de dar a conocer su contenido y que no cabe promover un uso abusivo de los datos personales publicados para otras finalidades.

Para ampliar información puede consultar los siguientes textos:

- Ley 30/1992, de Régimen Jurídico de las AAPP y del Procedimiento Administrativo Común. Arts.60 y 61.
- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 11.
- MBP Entidades Locales. Art. 51.

109 NO ES NECESARIO EL CONSENTIMIENTO DE LAS PERSONAS PARA REALIZAR UNA PUBLICACIÓN PRECEPTIVA QUE INCLUYE DATOS PERSONALES, CUYO OBJETIVO ES ALGUNO DE LOS SIGUIENTES: ASEGURAR UN LLAMAMIENTO, LA PRESENCIA DE PERSONAS INTERESADAS EN UN PROCEDIMIENTO O EL CUMPLIMIENTO DE UN DEBER LEGAL

- La técnica para asegurar el llamamiento o la presencia de las personas interesadas en un procedimiento es la publicación oficial del acto administrativo que les afecta; esta publicación puede hacerse en tablones de anuncios, boletines oficiales, páginas web y en los medios de comunicación.

- Cabe plantearse si es exigible el consentimiento de las personas interesadas para la publicación preceptiva de sus datos en distintos supuestos, tales como la concesión de licencias de apertura de establecimientos, notificación de deudas tributarias o de sanciones de tráfico por impagos o por no haberse podido practicar la notificación de manera personal. En estos casos, la publicidad viene impuesta normativamente por razones de transparencia (supuestos de concesión de licencias de apertura de establecimientos), para responder a la necesidad de asegurar el efecto útil del procedimiento (notificación de deudas tributarias), o se pretende obtener un efecto ejemplarizante (publicación de sanciones de tráfico).

- Por tanto, no será preciso el consentimiento de la persona afectada porque la publicación responde al cumplimiento a un deber legal.

Para ampliar información puede consultar los siguientes textos:

- Ley 30/1992, de Régimen Jurídico de las AAPP y del Procedimiento Administrativo Común. Arts. 58 a 61.
- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 6.2.

110

¿SE PUEDEN PUBLICAR EN INTERNET LAS ACTAS DE LOS PLENOS MUNICIPALES Y DE LAS REUNIONES DE LA JUNTA DE GOBIERNO LOCAL CUANDO ÉSTAS CONTIENEN DATOS DE CARÁCTER PERSONAL?

- Las actas de los plenos municipales se pueden publicar en internet, sin consentimiento de las personas cuyos datos aparecen en las mismas, si se dan dos condiciones: que así lo determine expresamente el Reglamento Orgánico de la entidad local y que la información con datos de carácter personal que contengan no afecte al honor, ni a la intimidad personal o familiar ni a la propia imagen de las personas afectadas.

- Las sesiones de los plenos de las corporaciones locales generalmente son públicas, salvo en aquellos asuntos que puedan afectar al derecho fundamental de los ciudadanos si así se acuerda por mayoría absoluta. Sin embargo, las sesiones de la Junta de Gobierno Local no son públicas y por ello sus actas no pueden publicarse en internet.

- La exposición pública y resumida de las actas de los plenos municipales, cualquiera que sea el medio a través del cual se realice, tiene como finalidad ofrecer una información genérica a los vecinos y a las vecinas y no tiene por qué ser una práctica informativa contraria a la normativa sobre protección de datos. Ahora bien, se aconseja eliminar de este resumen aquellos datos de carácter personal que no sean adecuados, pertinentes o que resulten excesivos y, por supuesto, datos personales especialmente protegidos.

- En los supuestos en que se autorice la grabación, por medio de imágenes y/o sonidos, de las sesiones que celebre el pleno municipal de la entidad local, esta grabación, y su correspondiente difusión, se suspenderá o limitará durante el tiempo que dure el debate de asuntos que puedan afectar al derecho a la intimidad personal o familiar.

Para ampliar información puede consultar los siguientes textos:

- Ley 7/1985, Reguladora de Bases de Régimen Local. Art.70.
- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Arts.7 y 11. 2 a.
- Real Decreto 2568/1986, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídica de Entidades Locales. Art. 229.2.
- MBP Entidades Locales. Art. 53.

111 PROCEDIMIENTOS SANCIONADORES Y PUBLICACIÓN DE DATOS PERSONALES

- En procedimientos sancionadores la publicación de los acuerdos adoptados viene impuesta en las normas reguladoras del procedimiento y, por tanto, no es necesario el consentimiento previo de la persona afectada.

- No obstante, en la publicación de los datos personales deben adoptarse las medidas necesarias para identificar, de manera objetiva, a la persona afectada, pero sin que esta publicación suponga una invasión de su esfera privada ni una actividad informativa de la administración que pueda describirse como desproporcionadamente amplia. Por ejemplo, mediante la mención de la referencia a un número de expediente de modo que no sea necesario hacer constar el motivo concreto de la infracción ni de la sanción impuesta.

Para ampliar información puede consultar los siguientes textos:

- Ley 30/1992, de Régimen Jurídico de las AAPP y del Procedimiento Administrativo Común. Arts. 58 a 61.
- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 6.2.

112 ¿QUÉ CAUTELAS DEBEN SEGUIRSE CUANDO LOS CONCEJALES Y CONCEJALAS, EN SU LABOR DE CONTROL, SOLICITAN DATOS PERSONALES?

- Los miembros de una corporación municipal tienen derecho a solicitar y obtener de la Presidencia cualquier información (cualitativa, cuantitativa, antecedentes, datos personales, etc.), siempre que obre en poder de los servicios de la entidad local y resulte necesaria para el desarrollo de su función de fiscalización y control de los órganos de gobierno de la entidad local.

- Las entidades locales establecerán un procedimiento para el ejercicio de este derecho; el procedimiento deberá incluir la forma y modelos de solicitud y de respuesta.

- Cuando la información solicitada incluya datos de carácter personal, se deberá valorar, en primer lugar, si es posible proceder a su disociación, sin que ello afecte al derecho de recibir la información necesaria para el ejercicio de las funciones de control.

- Si en la información suministrada a los concejales se facilitan datos personales y no se aplican técnicas de disociación, en el modelo de entrega de documentación se les recordará que deben observar el deber de confidencialidad de la información y, en particular, el deber de secreto respecto a los datos de carácter personal a los que acceden en el ejercicio de su cargo representativo, y que estos deberes subsisten aún después de finalizado su mandato.

- Los datos facilitados no pueden ser utilizados para funciones diferentes a las de control de los órganos de gobierno.

Para ampliar información puede consultar los siguientes textos:

- Ley 7/1985, Reguladora de Bases de Régimen Local. Art. 77.
- MBP Entidades Locales. Art. 52.
- Dictamen AVPD CN05-022.

113 ¿QUÉ CAUTELAS DEBEN SEGUIRSE CUANDO SE MENCIONAN DATOS DE CARÁCTER PERSONAL EN LOS PLENOS MUNICIPALES?

- Las sesiones del pleno de las corporaciones locales son públicas.
- No obstante, el debate y la votación de aquellos asuntos que puedan afectar al derecho fundamental de los ciudadanos al honor, la intimidad personal y familiar y a la propia imagen (artículo 18.1 de la Constitución) pueden ser secretos, siempre que lo acuerde el pleno por mayoría absoluta.

Para ampliar información puede consultar los siguientes textos:

- Ley 7/1985, Reguladora de Bases de Régimen Local. Art. 70.
- MBP Entidades Locales. Art. 52.
- Dictamen AVPD CN06-015.

114 ¿QUÉ CAUTELAS DEBEN SEGUIRSE RESPECTO DE LOS DATOS DE CARÁCTER PERSONAL EN LA EXPOSICIÓN PÚBLICA Y RESUMIDA DE LAS ACTAS?

- Las sesiones de los plenos de las corporaciones locales generalmente son públicas, salvo en aquellos asuntos que puedan afectar al derecho fundamental de los ciudadanos si así se acuerda por mayoría absoluta.
- La exposición pública y resumida de las actas del pleno, cualquiera que sea el medio a través del cual se realice, tiene como finalidad ofrecer una información genérica a los vecinos y a las vecinas y no tiene por qué ser una práctica informativa contraria a la normativa sobre protección de datos. Ahora bien, se aconseja eliminar de este resumen aquellos datos de carácter personal que no sean adecuados, pertinentes o que resulten excesivos y, por supuesto, datos personales especialmente protegidos.

Para ampliar información puede consultar los siguientes textos:

- Ley Reguladora de Bases de Régimen Local. Art. 70.
- MBP Ayuntamientos. Art. 53.
- Dictamen AVPD CN 06-015.

115

¿QUÉ CAUTELAS DEBEN SEGUIRSE CUANDO SE GRABEN Y DIFUNDAN LOS PLENOS O TRABAJOS EN COMISIÓN A TRAVÉS DE TELEVISIONES LOCALES O INTERNET?

- En los supuestos en que se autorice la grabación, por medio de imágenes y/o sonidos, de las sesiones que celebre el pleno municipal de la entidad local, esta grabación, y su correspondiente difusión en internet o en televisiones locales, se suspenderá o limitará durante el tiempo que dure el debate de asuntos que puedan afectar al derecho a la intimidad personal o familiar y a la propia imagen.

Para ampliar información puede consultar los siguientes textos:

- Ley 7/1985, Reguladora de Bases de Régimen Local. Art. 70.
- MBP Entidades Locales. Art. 53.
- Dictamen AVPD CN06-015.

116 CON RELACIÓN A LA ADJUDICACIÓN DE VIVIENDAS ¿PUEDEN EXPONER LOS AYUNTAMIENTOS LAS LISTAS PROVISIONALES, LAS DEFINITIVAS, LAS ADJUDICACIONES Y LAS LISTAS DE ESPERA EN LA OFICINA DE SERVICIO A LA CIUDADANÍA?

- Sí, si pueden. La adjudicación de las VPO debe llevarse a cabo respetando los principios de publicidad, concurrencia y transparencia, según dispone la Orden de 14 de junio de 2002, del Consejero de Vivienda y Asuntos Sociales, que regula el procedimiento de adjudicación de viviendas de protección oficial.

- En consecuencia, la publicación es necesaria por razones de transparencia, así como para facilitar a la ciudadanía el que pueda recurrir el acto administrativo de la adjudicación, de conformidad con lo dispuesto en la norma arriba citada.

- Igualmente se dispone que la lista de personas admitidas y excluidas y de adjudicatarias y la correspondiente lista de espera conformada por todas las personas que no hayan resultado agraciadas será objeto de la oportuna publicación.

- Por otra parte, el artículo 55 de la LBRL establece que, para la efectividad de la coordinación y eficacia administrativa, el Estado, las comunidades autónomas y las entidades locales, en sus relaciones recíprocas, deberán prestar activamente la cooperación y la asistencia que las otras administraciones pudieran precisar para el eficaz cumplimiento de sus fines.

- Una forma de cooperación y asistencia puede ser la publicación en el tablón de anuncios del ayuntamiento de las listas provisionales, las definitivas, las adjudicaciones de viviendas, etc. cuando así se lo requieren otras administraciones.

Para ampliar información puede consultar los siguientes textos:

- Orden del 14 de junio de 2002, del Consejero de Vivienda y Asuntos Sociales sobre procedimiento de adjudicación de VPO.
- Ley Reguladora de Bases de Régimen Local. Art. 55.

117 CON RELACIÓN A LA ADJUDICACIÓN DE VIVIENDAS ¿PUEDEN EXPONER LOS AYUNTAMIENTOS LAS LISTAS PROVISIONALES, LAS DEFINITIVAS Y LAS ADJUDICACIONES Y LAS LISTAS DE ESPERA EN SITIO WEB DEL AYUNTAMIENTO?

- Sí, si pueden. La adjudicación de las VPO debe llevarse a cabo respetando los principios de publicidad, concurrencia y transparencia, según dispone la Orden de 14 de junio de 2002, del Consejero de Vivienda y Asuntos Sociales, que regula el procedimiento de adjudicación de viviendas de protección oficial.

- En consecuencia, la publicación es necesaria por razones de transparencia, así como para facilitar a la ciudadanía el que pueda recurrir el acto administrativo de la adjudicación, de conformidad con lo dispuesto en la norma arriba citada.

- Igualmente se dispone que la lista de personas admitidas y excluidas y de adjudicatarias y la correspondiente lista de espera conformada por todas las personas que no hayan resultado agraciadas será objeto de la oportuna publicación.

- Por otra parte, el artículo 55 de la LBRL establece que, para la efectividad de la coordinación y eficacia administrativa, el Estado, las comunidades autónomas y las entidades locales, en sus relaciones recíprocas, deberán prestar activamente la cooperación y la asistencia que las otras administraciones pudieran precisar para el eficaz cumplimiento de sus fines.

- Una forma de cooperación y asistencia puede ser la publicación en la página web del ayuntamiento de las listas provisionales, las definitivas, las adjudicaciones de viviendas, etc. cuando así se lo requieren otras administraciones.

Para ampliar información puede consultar los siguientes textos:

- Orden del 14 de junio de 2002, del Consejero de Vivienda y Asuntos Sociales, sobre procedimiento de adjudicación de VPO.
- Ley Reguladora de Bases de Régimen Local. Art. 55.

118 EN LOS LISTADOS DE GESTIÓN DE LOS PROCESOS DE ADJUDICACIÓN DE VIVIENDA SE INCLUIRÁ SÓLO EL NOMBRE Y DOS APELLIDOS ¿ES POSIBLE INCLUIR EL DNI O ES MÁS ADECUADO INDICAR DATOS NO PERSONALES, TALES COMO NÚMERO DE EXPEDIENTE, NÚMERO ASIGNADO PARA EL SORTEO, ETC.?

- Respecto al contenido de la publicación de los datos de las personas participantes en un proceso de adjudicación de viviendas de protección oficial, el artículo 8.2. de la Orden de 14 de junio de 2002, del Consejero de Vivienda y Asuntos Sociales, que regula el procedimiento de adjudicación de viviendas de protección oficial, establece la publicación de los siguientes datos: nombre y DNI de las personas solicitantes, la composición de la unidad convivencial y la especificación de la reserva o cupo en que se ha clasificado la solicitud. Además, en el caso de personas discapacitadas, con movilidad reducida de carácter permanente, se especificará en qué baremo se clasifica la solicitud.

- En consecuencia, sí es posible incluir el DNI. Sin embargo, no es una buena práctica administrativa, pues resulta muy invasiva con relación a la esfera privada de las personas y es claramente desproporcionada respecto al logro del efecto útil del procedimiento.

- La publicidad pretendida puede lograrse con la publicación sólo del nombre y los apellidos de las personas interesadas, sin necesidad de publicar el DNI ni el domicilio, etc.

- De otra parte, la Orden citada obvia la cuestión de que el dato referido a personas con discapacidades, que optan a una VPO, es un dato personal especialmente protegido, según el artículo 7 de la LOPD. Esto es así porque la discapacidad está relacionada con la salud de las personas.

- En base a las anteriores normas, se concluye que en la publicación no debe especificarse cuál es la discapacidad que una persona tiene reconocida ni su grado, ya que esta información no resulta proporcional respecto al cumplimiento de la finalidad del procedimiento de adjudicación de las viviendas de protección oficial.

Para ampliar información puede consultar los siguientes textos:

- Orden del 14 de junio de 2002, del Consejero de Vivienda y Asuntos Sociales sobre procedimiento de adjudicación de VPO.
- Ley Orgánica 15/1999. Art. 7.
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Art. 81.6.

119 ¿PUEDE LA POLICÍA MUNICIPAL ACCEDER A LOS DATOS DE LA DIRECCIÓN GENERAL DE TRÁFICO? ¿CUÁL ES LA FINALIDAD DE ESTE ACCESO? ¿ES UNA CESIÓN DE DATOS?

- La Dirección General de Tráfico tiene atribuida la responsabilidad de los registros de personas y vehículos.
- Un ayuntamiento tiene la competencia para la recaudación del impuesto sobre vehículos de tracción mecánica y se atribuye a los alcaldes la competencia sancionadora sobre las infracciones a las normas de circulación cometidas en vías urbanas.
- El Reglamento General de Vehículos permite el acceso al registro de vehículos por parte de terceros, siempre que se acredite un interés legítimo y directo. Este interés resulta reforzado en los supuestos de las relaciones entre las administraciones públicas, dados los principios que las informan y que están contenidos en el art. 4 de la Ley 30/1992 y en el art. 21.1 de la LOPD, que permite la comunicación de datos personales entre las administraciones públicas cuando ejerzan competencias que versen sobre la misma materia, en este caso, la sancionadora por hechos de tráfico.
- En consecuencia, sí se trata de una cesión o comunicación de datos entre administraciones públicas para el ejercicio de competencias que versan sobre la misma materia.

Para ampliar información puede consultar los siguientes textos:

- Real Decreto 1449/2000, por el que se modifica y desarrolla la estructura orgánica básica del Ministerio del Interior.
- Ley 7/1985, Reguladora de Bases de Régimen Local. Arts. 15 y ss.
- Real Decreto Legislativo 2/2004, por el que se aprueba el texto refundido de la Ley Reguladora de las Haciendas Locales. Título II.
- Real Decreto Legislativo 339/1990, Ley sobre Tráfico, Circulación a Motor y Seguridad Vial. Art. 68.
- Real Decreto 2822/1998, Reglamento General de Vehículos.
- Ley 30/1992, de Régimen Jurídico de las AAPP y del Procedimiento Administrativo Común. Art. 4.
- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 21.1.

120 ¿PUEDE LA POLICÍA LOCAL CEDER DATOS PERSONALES RELACIONADOS CON ACCIDENTES DE CIRCULACIÓN A COMPAÑÍAS ASEGURADORAS?

- Sí. Es una de las excepciones, recogidas en la Ley, a la necesidad de solicitar el consentimiento para la cesión de datos personales. El responsable del fichero donde se recogen datos de accidentes de circulación puede facilitar los datos personales recogidos a las compañías de seguros que actúen en calidad de parte interesada en el mismo.

- Con carácter previo a la cesión, es imprescindible que las compañías aseguradoras acrediten la representación de sus asegurados y que éstos tengan un interés legítimo y directo en el accidente, respecto al cual se solicita la información que dispone la policía local.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Arts. 11. 2 a. y c.
- Real Decreto 1428/2003, Reglamento de Circulación. Art. 129.
- Ley 30/1992, de Régimen Jurídico de las AAPP y del Procedimiento Administrativo Común. Art. 35.

121 ¿PUEDE LA POLICÍA MUNICIPAL ACCEDER A LOS DATOS PERSONALES DE MENORES ESCOLARIZADOS EN UN CENTRO EDUCATIVO DE LA LOCALIDAD?

- La policía local puede efectuar diligencias de prevención y actuaciones para evitar la comisión de actos delictivos, en el marco de la colaboración establecida en las Juntas de Seguridad.

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

- El responsable del fichero de datos personales de los menores, en este caso el centro escolar, ha de responder a la solicitud de información de la policía local, siempre que la petición se realice de forma concreta y específica, puesto que no es adecuado realizar solicitudes masivas de datos.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 2/1986, Reguladora de las Fuerzas y Cuerpos de Seguridad del Estado, de las Policías de las Comunidades Autónomas y de las Policías Locales.
- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 22.

122 ¿ES ADECUADO QUE UN CENTRO EDUCATIVO ELABORE UN INFORME, A PETICIÓN DE LA POLICÍA LOCAL, PARA VALORAR LA SITUACIÓN SOCIO-FAMILIAR DE UN MENOR?

- La policía municipal no puede, a iniciativa propia, solicitar a los centros educativos, informes sobre los menores, para valorar una potencial situación de desamparo. En todo caso, si tiene constancia de tal situación, deberá comunicarlo a la Comisión de Tutela del Menor.

- Las autoridades y los servicios públicos tienen las siguientes obligaciones: prestar, de forma inmediata, la atención que precise cualquier menor; para lograr lo anterior están obligadas a actuar, si corresponde a su ámbito de competencias, o dar traslado, en otro caso, al órgano competente, y, finalmente, están obligadas a poner los hechos en conocimiento de los representantes legales del menor, o cuando sea necesario, del Ministerio Fiscal.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 1/1996, de Protección Jurídica del Menor. Arts.14, 16 y 18.
- Código Civil. Art. 172.

123 ¿DEBEN DECLARARSE A LA AGENCIA VASCA DE PROTECCIÓN DE DATOS LOS SISTEMAS DE VIDEOVIGILANCIA INSTALADOS EN EDIFICIOS MUNICIPALES?

- Las imágenes de personas captadas o grabadas por cámaras o videocámaras deben ser consideradas datos de carácter personal, de acuerdo con la definición de la LOPD en su artículo 3 a): ”cualquier información concerniente a personas físicas identificadas o identificables”.

- Más concretamente, el artículo 5.1 f) del RD 1720/2007, que desarrolla la LOPD, considera datos de carácter personal a “cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a persona físicas identificadas o identificables”.

- Los sistemas de videovigilancia instalados en edificios municipales pueden estar sometidos a dos sistemas de control diferentes:
  - Si son sistemas de videovigilancia utilizados por cuerpos y fuerzas de seguridad, tienen un régimen específico de autorización previa. Asimismo, en su instalación y uso deben respetarse una serie de principios, de criterios de conservación y de atención respecto del ejercicio de derechos por los ciudadanos. Todo ello está regulado en la Ley Orgánica 4/1997, sobre utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos y en el Decreto 168/1998, que la desarrolla para la Comunicad Autónoma del País Vasco.
  - Si los sistemas de videovigilancia no son utilizados por cuerpos y fuerzas de seguridad, están sometidos a la normativa de protección de datos personales. En consecuencia, los ficheros que identifiquen las grabaciones realizadas por estas videocámaras deberán crearse e inscribirse en el Registro de Protección de Datos de Euskadi. Asimismo, deberán respetarse los principios, las obligaciones y las medidas de seguridad previstas en la normativa en materia de protección de datos.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.
  Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD.
- INSTRUCCIÓN 1/2006, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

- Ley Orgánica 4/1997, sobre utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.
- Decreto 168/1998, por el que se desarrolla el régimen de autorización y utilización de videocámaras por la Policía del País Vasco en lugares públicos.

124 ¿CÓMO SE DEBE AVISAR E INFORMAR DE LA EXISTENCIA DE SISTEMAS DE VIDEOVIGILANCIA?

- Cuando se trata de sistemas de videovigilancia utilizados por cuerpos y fuerzas de seguridad, se ha de informar al público, de manera clara y permanente, de la existencia de videocámaras fijas, sin especificar su emplazamiento, así como de la autoridad competente de la que dependen.

- Cuando se trate de sistemas de videovigilancia no utilizados por cuerpos y fuerzas de seguridad, están sometidos al régimen general de protección de datos personales. En este supuesto, se deberá cumplir con el deber de información previsto en el artículo 5 de la LOPD. A tal fin, se deben colocar en las zonas vídeo vigiladas distintivos informativos, ubicados en un lugar suficientemente visible, tanto en espacios abiertos como cerrados. En estos distintivos se informará sobre:
  - Cuál es la zona que está sometida a videovigilancia.
  - A qué persona se puede solicitar información adicional. Para ello, deberán ponerse a disposición de los interesados impresos en los que se detalle la información prevista en el artículo 5.1 de la LOPD, esto es, información sobre el fichero y el tratamiento, su finalidad y los destinatarios de la información, etc.
  - Ante quién se pueden ejercer los derechos de acceso, rectificación, cancelación y oposición al tratamiento de los datos personales.

- En el sitio web de la AVPD existe un modelo de distintivo informativo para avisar sobre la existencia de sistemas de videovigilancia.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD.
- INSTRUCCIÓN 1/2006, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

- Ley Orgánica 4/1997, sobre utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.
- Decreto 168/1998, por el que se desarrolla el régimen de autorización y utilización de videocámaras por la Policía del País Vasco en lugares públicos.

125 ¿SE DEBE FACILITAR EL ACCESO A UN EXPEDIENTE DE URBANISMO EN TRAMITACIÓN A LA PERSONA QUE ACREDITE LA CONDICIÓN DE INTERESADA?

- Sí, se debe facilitar. El derecho de acceso reconocido en el artículo 35. a) de la LRJPAC, es una facultad esencial de la que se disfruta si se tiene la condición de persona interesada, esto es, si se tiene un interés legítimo en un determinado procedimiento administrativo, y cuyo ejercicio tiene verdadero sentido mientras dicho procedimiento se encuentra en tramitación.

Para ampliar información puede consultar los siguientes textos:

- Ley 30/1992, de Régimen Jurídico de las AAPP y del Procedimiento Administrativo Común. Art. 35.a.
- MBP Entidades Locales. Art. 48.1.

126 ¿SE DEBE FACILITAR COPIA COMPLETA DEL EXPEDIENTE MEDIOAMBIENTAL EN TRÁMITE A CUALQUIER PERSONA QUE LO SOLICITE?

- Sí. La Ley 38/1995, de 12 de diciembre, regula el derecho de acceso a la información en materia de medio ambiente y declara que las administraciones públicas publicarán información de carácter general sobre el estado del medio ambiente de forma periódica.

- A su vez, la Directiva 2003/4/CE, del Parlamento Europeo y del Consejo, de fecha 28 de enero de 2003, relativa al acceso del público a la información medioambiental, amplía el marco de la información a suministrar no sólo a aquélla que, perteneciente a sus funciones, obra en su poder, sino también a la información de la que en su nombre disponga otra entidad, con vistas a su difusión activa y sistemática al público, particularmente por medio de la tecnología de telecomunicación informática o electrónica.

- En aplicación de la citada normativa se entiende por información urbanística y medioambiental toda la información disponible por las administraciones públicas bajo cualquier forma de exposición y en todo tipo de soporte material, referida a los instrumentos de planeamiento y gestión urbanística y a la situación urbanística de los terrenos, así como a las actividades y medidas que puedan afectar a la misma.

- El derecho de acceso a la información urbanística se ejerce sin necesidad de acreditar un interés determinado.

Para ampliar información puede consultar los siguientes textos:

- Ley 38/1995, de acceso a la información en materia de medio ambiente.
- Directiva 2003/4/CE, del Parlamento Europeo y del Consejo, de acceso del público a la información medioambiental.

127 ¿CUÁLES SON LOS FICHEROS Y LOS DATOS PERSONALES QUE LAS ENTIDADES LOCALES SUELEN GESTIONAR PARA REALIZAR LA ADMINISTRACIÓN DE PERSONAL Y LA DIRECCIÓN DE LAS PERSONAS?

- Fichero de Recursos Humanos o RRHH: datos identificativos (apellidos, nombre, y DNI), datos relativos a la vida laboral (puestos desempeñados, cursos impartidos y otros aspectos como competencias y capacidades demostradas, etc.), datos formativos (titulaciones y grados académicos, formación continua y cursos de especialización), datos de la relación administrativa (relación de empleo, situación administrativa, puntuaciones obtenidas en los procesos de selección y provisión, datos de licencias y permisos con las fechas de disfrute, etc.).

- Fichero de Seguridad Social o datos económicos: retribuciones, retenciones de impuestos, cotizaciones a Seguridad Social, domicilio, estado civil, número de hijos, afiliación sindical y descuento de cuota sindical, discapacidades de hijos, obligación de pagar pensión por resolución judicial, número de cuenta de entidad bancaria, número de días de baja (si ha sido enfermedad común o profesional), etc.

- Fichero de datos de Salud o del servicio médico: datos de salud laboral, revisiones médicas, discapacidades.

- Otros ficheros y datos: datos biométricos para el control horario, datos de vigilancia del correo electrónico, datos de vigilancia de acceso a internet, etc.

128 ¿DEBE RECABARSE EL CONSENTIMIENTO PREVIO DE LAS PERSONAS BENEFICIARIAS ANTES DE CONTRATAR PÓLIZAS DE SEGURO COLECTIVAS O PLANES DE PENSIONES?

- Cuando la entidad local suscribe una póliza de seguros o un plan de pensiones, como consecuencia de lo acordado en el convenio colectivo o en el acuerdo de condiciones laborales, y tiene que ceder datos personales a la entidad, aseguradora o previsora, según sea el caso, no es necesario solicitar consentimiento previo del trabajador, aunque sí informarle de la cesión realizada.

- En el supuesto de que la suscripción de una póliza o de un plan de pensiones no hayan sido acordados en el convenio colectivo o en el acuerdo de condiciones de trabajo, será necesario solicitar el consentimiento previo.

129 ¿SE REQUIERE EL CONSENTIMIENTO DE LAS PERSONAS AFECTADAS PARA LA CESIÓN DE DATOS QUE DEBE PRACTICARSE A LAS HACIENDAS FORALES EN MATERIA DE IRPF?

- No se requiere el consentimiento de las personas afectadas porque la cesión está autorizada en la normativa tributaria de aplicación a las haciendas forales.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 11.
- Normativa tributaria acerca del Impuesto sobre la Renta de las personas físicas y, en particular, lo referente a retenciones e ingresos a cuenta a favor de las Haciendas Locales. En concreto, a modo de ejemplo, para el Territorio Histórico de Álava: la Norma Foral 3/2007, y la Orden Foral 651/2007, sobre Impuesto sobre la renta de las personas físicas.

130 ¿SE REQUIERE EL CONSENTIMIENTO DE LAS PERSONAS AFECTADAS PARA LA CESIÓN DE DATOS A LA *TESORERÍA GENERAL DE LA SEGURIDAD SOCIAL*, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES QUE INCUMBEN A LAS ENTIDADES LOCALES?

- No se requiere el consentimiento de las personas afectadas porque la cesión está autorizada en la normativa de la seguridad social.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 11.
- Normativa de Inscripción y afiliación a la seguridad social y, en particular, el RD 84/1996, por el que se aprueba el Reglamento General sobre inscripción de empresas y afiliación, altas, bajas y variaciones de datos de trabajadores en la Seguridad Social.

131 ¿ES NECESARIO RECABAR EL CONSENTIMIENTO PREVIO DE LAS PERSONAS TRABAJADORAS PARA LA COMUNICACIÓN DE DATOS PERSONALES A SUS REPRESENTANTES?

- No se requiere el consentimiento de las personas trabajadoras en los supuestos que están contemplados en las leyes, principalmente en el Estatuto de los Trabajadores.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 11.
- Estatuto de los Trabajadores. Art. 64.

132 ¿QUÉ DATOS RELATIVOS A LAS PERSONAS TRABAJADORAS PUEDEN CEDERSE AL COMITÉ DE EMPRESA O A LA JUNTA DE PERSONAL?

- Pueden contemplarse estos supuestos:
  - Información trimestral de la situación de la empresa u organización en su sector económico.
  - Copia básica de los contratos.
  - Información económica sobre la marcha de la empresa: balance, cuenta de resultados, memoria y documentos de la sociedad.
  - Información para poder emitir un informe previo sobre plantillas de puestos, reducciones de jornada, traslado de instalaciones, planes de formación, implantación de sistemas de organización y control del trabajo, vigilancia del cumplimiento por parte del empresario de la normativa laboral, de seguridad social y de seguridad e higiene en el trabajo.
  - Información para poder emitir un informe sobre absorción, fusión o modificación de estatus de la empresa.
  - Información sobre la incidencia del empleo en la empresa.
  - Información sobre el censo de electores.
- En muchos casos, es suficiente proporcionar sólo datos disociados, esto es, datos que no permiten la identificación de la persona afectada o interesada, para cumplir el mandato legal de informar.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 11.
- Estatuto de los Trabajadores. Art. 64.

133 ¿EXISTEN LÍMITES A RESPETAR EN LA PUBLICACIÓN DEL CENSO ELECTORAL DE LAS PERSONAS TRABAJADORAS, CON MOTIVO DE LA CELEBRACIÓN DE ELECCIONES SINDICALES?

- El censo de electores se ha de trasladar a los miembros de las mesas electorales e incluye los siguientes datos: apellidos, nombre y fecha de nacimiento.
- Las mesas electorales harán público el censo mediante alguno de los siguientes sistemas de difusión: tablones de anuncios y/o intranet. En ningún caso, se debe publicar el censo electoral en un sitio web de acceso abierto o no restringido.
- Aún cuando no se contempla expresamente la cesión del censo electoral a los sindicatos, es lógico interpretar que es necesario hacerlo para que cada sindicato pueda realizar la campaña sindical previa a las elecciones.
- En este supuesto de cesión del censo electoral a los sindicatos previo a las elecciones, el principio de calidad implica que los sindicatos no podrán utilizarlo para finalidades distintas a la organizar la campaña electoral y que deberán cancelar la información una vez finalizada la campaña sindical.

Para ampliar información puede consultar los siguientes textos:

- Dictamen AVPD CN06-029.

134 ¿ES NECESARIO EL CONSENTIMIENTO DE LAS PERSONAS TRABAJADORAS PARA QUE UNA ENTIDAD LOCAL ORGANICE LA REALIZACIÓN DE UN RECONOCIMIENTO MÉDICO DE SUS EMPLEADOS?

- Sí, es necesario el consentimiento previo de las personas trabajadoras excepto en los siguientes supuestos: a) cuando el reconocimiento sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores, b) cuando se busca verificar si el estado de salud de un trabajador puede constituir un peligro para el mismo o para sus compañeros trabajadores o para otras personas relacionadas con la empresa, y c) cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad. En todos estos supuestos se requiere informe previo de los representantes de los trabajadores.

- Si las acciones de vigilancia de la salud son obligatorias o, si son voluntarias y la persona trabajadora ya ha prestado su consentimiento para someterse a las mismas, no será preciso exigir un consentimiento adicional para el tratamiento de sus datos de salud.

- En cualquiera de los casos, ha de cumplirse el deber de información, esto es, hay que informar a los trabajadores de cuál es la finalidad para la cual se recogen sus datos personales (de salud, de identificación, etc.), en qué fichero se guardarán, quién es el responsable de ese fichero, cuáles son sus derechos, si se van a comunicar sus datos a otras personas y entidades y, en caso afirmativo, cuáles son éstas, etc.

Para ampliar información puede consultar los siguientes textos:

- Ley 31/1995, de Prevención de Riesgos Laborales. Art. 22.1.
- Informe AEPD 434-2004.

135 ¿QUÉ CAUTELAS ESPECIALES SE HAN DE OBSERVAR RESPECTO DE LOS DATOS DE SALUD DE LOS TRABAJADORES?

- La entidad local recoge datos de salud de sus empleados para poder cumplir con sus obligaciones en materia de seguridad y salud laboral.

- La entidad local tiene la obligación legal de crear un servicio de prevención, que asume responsabilidades en prevención y protección de riesgos. Alternativamente, la entidad local puede contratar estos servicios con una Mutua de Accidentes de Trabajo y Enfermedades Profesionales.

- En este último caso, la entidad local ha de especificar en el contrato o convenio firmado con la Mutua lo estipulado en el artículo 12 de la LOPD, relativo al acceso a los datos por cuenta de terceros, en concreto: cómo la mutua tratará los datos personales conforme a las instrucciones del responsable del tratamiento, que no los utilizará para un fin distinto al que figure en el contrato, ni los comunicará a otras personas, así como las medidas de seguridad que está obligada a implementar.

- Se ha de crear un fichero específico para recoger los datos de salud de los trabajadores. Estos datos de salud son especialmente protegidos.

- El acceso a los datos de salud de los trabajadores está restringido a los profesionales sanitarios de la entidad local o de la mutua y al propio trabajador. En supuestos concretos, se puede ceder información a los delegados de prevención del Comité de Seguridad e Higiene, si bien generalmente se facilitarán datos agregados o sociales y sólo excepcionalmente datos personales.

Para ampliar información puede consultar los siguientes textos:

- Ley 31/1995, de Prevención de Riesgos Laborales.
- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Arts. 7 y 8.

136

¿REQUIERE CONSENTIMIENTO PREVIO DE LOS TRABAJADORES LA CESIÓN DE DATOS A LA MUTUA DE ACCIDENTES DE TRABAJO Y ENFERMEDADES PROFESIONALES COLABORADORA DE LA SEGURIDAD SOCIAL?

- Las Mutuas de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social podrán desarrollar para las empresas las funciones correspondientes a los servicios de prevención y protección de riesgos, siempre y cuando hayan sido objeto de acreditación por la autoridad laboral.

- La Mutua que tenga encomendado este servicio tiene la condición de encargada de tratamiento y la entidad local tiene que firmar con ella un contrato por escrito, en el que se especifica lo estipulado en el artículo 12 de la LOPD, relativo al acceso a los datos por cuenta de terceros, en concreto: cómo la mutua tratará los datos personales conforme a las instrucciones del responsable del tratamiento, que no los utilizará para un fin distinto al que figure en el contrato, ni los comunicará a otras personas, así como las medidas de seguridad que está obligada a implementar. Como consecuencia de este encargo de tratamiento, pueden trasladarse datos personales entre la entidad local y la mutua.

- Las mutuas pueden comunicar a la entidad local sólo el informe de aptitud psicofísica del empleado; al servicio médico de la entidad sí pueden enviarle datos médicos. Finalmente, los informes médicos han de ser comunicados únicamente a los trabajadores y es responsabilidad de la mutua garantizar la confidencialidad y seguridad en las comunicaciones con los empleados de la entidad.

Para ampliar información puede consultar los siguientes textos:

- Ley 31/1995, de Prevención de Riesgos Laborales. Art. 32.

137 ¿SE PUEDEN UTILIZAR DATOS BIOMÉTRICOS PARA EL CONTROL DE ACCESO DE LOS EMPLEADOS A LA ENTIDAD LOCAL?

- Con una frecuencia creciente se utilizan sistemas de control de acceso y presencia de los empleados basados en datos biométricos, fundamentalmente a través de la huella digital y, en menor medida, mediante el contorno de manos, el iris, etc.

- El uso de datos biométricos con la finalidad de controlar la presencia física ha sido una cuestión controvertida; en la actualidad, los tribunales de justicia consideran que se trata de un uso legítimo.

Para ampliar información puede consultar los siguientes textos:

- Sentencias Tribunal Superior de Cantabria de 23 de enero de 2003 y de 21 febrero 2003.

138 ¿QUÉ PRÁCTICAS DE SOLICITUD DE DATOS PERSONALES SON INADECUADAS EN LOS PROCESOS DE SELECCIÓN?

- La entidad local tiene que ser capaz de evaluar si las personas que va a contratar son trabajadoras aptas para el desempeño de los puestos y seleccionar de entre ellas a las idóneas, en función de su mérito y capacidad.

- Como norma general, es necesario pedir el consentimiento previo de la persona antes de solicitar sus datos personales. Ahora bien, la cumplimentación de una instancia de solicitud de participación en un proceso selectivo supone un consentimiento inequívoco de la persona a la recogida de sus datos personales, siempre que los datos que se pretendan obtener puedan valorarse como adecuados, pertinentes y no excesivos con relación a la finalidad selectiva.

- En este sentido, es preciso evitar algunas prácticas selectivas de solicitud de información personal que puedan suponer un entrometimiento en la esfera privada de la persona, al recabar datos irrelevantes, esto es, no adecuados, no pertinentes y excesivos.

- A la hora de determinar la recolección mediante cuestionarios o entrevistas selectivas de datos personales, incluso de datos delicados o especialmente protegidos, es necesario evaluar que la información personal que se va a solicitar tiene una relación directa, soportada por la literatura científica, con la decisión a tomar en materia de empleo.

- Es difícil enumerar todos los tipos de datos que pueden manejarse con una finalidad selectiva, pues su identificación dependerá de las características del empleo. Parece más lógico enunciar reglas destinadas a garantizar la claridad de la operación y el conocimiento de la misma por la persona afectada. No obstante, en la mayoría de las ocasiones no es necesario preguntar a las personas acerca de su vida fuera del trabajo.

- Algunas prácticas INADECUADAS son:
  - Pedir más datos de los necesarios para evaluar la aptitud de los candidatos.
  - Solicitar los datos personales a terceras personas, sin el consentimiento del aspirante. Por ejemplo, recabar información sobre el rendimiento a un empleador anterior.
  - Realizar exámenes o preguntar por la salud a los candidatos para otros fines que no son determinar la aptitud para el puesto.

Para ampliar información puede consultar los siguientes textos:

- OIT/96/29 7 octubre 1996. Repertorio de recomendaciones prácticas sobre la protección de datos personales de los trabajadores.

139 ¿ES ADECUADO PUBLICAR EN INTERNET UNA GUÍA DE COMUNICACIÓN DE LA ENTIDAD LOCAL QUE INCLUYA, ADEMÁS DE LA IDENTIFICACIÓN DE LOS PUESTOS DE TRABAJO QUE DAN UN SERVICIO PÚBLICO, LOS DATOS DE IDENTIFICACIÓN DE SUS OCUPANTES?

- Las organizaciones quieren facilitar su comunicación con los ciudadanos. De ahí que las entidades públicas identifiquen sus unidades de servicio, los puestos de trabajo y los datos de contacto (correo electrónico, teléfono y dirección postal) y los publiquen en guías de comunicación, en formato papel y en formato electrónico.

- Respecto a la cuestión sobre la publicación, en particular en internet, también de los datos de identificación personal (entiéndase, el nombre y los apellidos) de las personas que ocupan los puestos de trabajo, esta práctica comunicativa ha originado frecuentemente conflictos entre los trabajadores y su entidad cuando no ha estado precedida de la solicitud del consentimiento previo a las personas para hacerlo.

- Desde un punto de vista práctico, esto es, para acercar la administración a un ciudadano y poder ofrecerle la información que necesite con prontitud, por ejemplo, con una simple llamada, no parece necesario, ni proporcional al fin pretendido, la publicación en internet de los datos personales de un funcionario. Máxime cuando, en ocasiones, la rotación de las personas en los puestos o su ausencia en períodos vacacionales o durante bajas laborales puede resultar en que haya que pensar en modificar, provisional o definitivamente, los datos personales publicados en internet.

- En cualquier caso, si una entidad local decidiera publicar una guía de comunicación incluyendo los datos identificativos de sus empleados, en virtud del artículo 2.2. del RD 1720/2007, por otro lado, de previsible aplicación restrictiva, parece que una práctica muy recomendable es solicitar a los trabajadores su consentimiento previo para hacerlo y explicitar en la publicación que la información no constituye una fuente de acceso público.

Para ampliar información puede consultar los siguientes textos:

- Estatuto del Empleado Público. Art. 74.
- Dictamen AVPD CN3/2007.
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Art. 2.2.

140 ¿QUÉ DATOS PERSONALES SE PUEDEN PUBLICAR EN LOS LISTADOS DE ASPIRANTES, CANDIDATOS O RESULTADOS, DERIVADOS DE LA GESTIÓN DE LOS PROCESOS SELECTIVOS O DE CONCURSOS DE TRASLADOS?

- En procesos selectivos o provisorios, los listados con datos personales (listas de admitidos, de puntuaciones, etc.) pueden tener una capacidad de difusión mayor (boletines en internet) o menor (intranet, internet con claves de acceso, tablones de anuncios en formato papel) en función de lo que establezca la convocatoria. Como norma general de respeto a la privacidad, los listados deberían contener los datos personales mínimos para cumplir el principio de publicidad.

- Además, los listados incorporarán una cláusula que advierta que contienen datos de carácter personal, que se ajustan a la legislación actual en materia de protección de datos y que su única finalidad es dar publicidad a la fase del proceso de que se trate y notificar lo que proceda a los participantes.

- Asimismo, incorporarán un párrafo informativo en el que se deje constancia de que estos listados no constituyen una fuente de acceso público y que no podrán ser reproducidos, ni en todo ni en parte, ni transmitidos ni registrados por ningún sistema de recuperación de información, sin el consentimiento de los propios afectados.

Para ampliar información puede consultar los siguientes textos:

- Dictámenes AVPD CN07-028 y CN07-036.

141 ¿ES LÍCITO EXAMINAR EL CONTENIDO DEL CORREO ELECTRÓNICO DE LOS TRABAJADORES DE UNA ENTIDAD LOCAL?

- El correo electrónico es una herramienta de trabajo que permite una comunicación inmediata, simplifica el trabajo y puede ayudar a gestionar de forma más eficiente el tiempo de trabajo.

- Existen técnicas para controlar y acceder a todos los correos electrónicos, tanto a los datos del envío y recepción como al contenido de los mensajes. Pero estas herramientas de control no se pueden usar indiscriminadamente en ninguna organización. La Constitución garantiza el secreto de las comunicaciones, en especial, de las postales, telegráficas y telefónicas. Por extensión se interpreta que el secreto del correo electrónico está amparado constitucionalmente.

- La vigilancia de los trabajadores no está prohibida pero ha de adoptar límites muy claros. En este sentido, sólo puede efectuarse si los trabajadores interesados han sido previamente informados acerca de las intenciones del empleador, esto es, no cabe el control secreto del uso del correo, salvo que existan sospechas razonablemente justificadas de actividades delictivas u otras infracciones graves. En consecuencia, antes de que se pongan en marcha las actividades de vigilancia, los trabajadores deben conocer las finalidades de ésta y saber con precisión en qué períodos se efectuará.

- Es conveniente llegar a acuerdos, en el marco del convenio colectivo o del acuerdo de condiciones laborales, en las cuales se establezcan protocolos de actuación para el uso del correo electrónico por parte de los trabajadores y, en su caso, sobre los sistemas de control por parte de la entidad local.

Para ampliar información puede consultar los siguientes textos:

- Constitución Española. Art. 18.3.
- Ley Orgánica 10/1995, del Código Penal. Art. 197.1.
- OIT/96/29. Repertorio de recomendaciones prácticas sobre la protección de datos personales de los trabajadores.

142 ¿ES LÍCITO EXAMINAR LAS PÁGINAS DE INTERNET VISITADAS POR LAS PERSONAS QUE TRABAJAN EN UNA ENTIDAD LOCAL?

- El acceso a internet, así como la aplicación de mecanismos para restringir los lugares electrónicos que pueden ser visitados, etc. es determinado por la entidad local.

- Existen técnicas para conocer y controlar los sitios electrónicos visitados por los trabajadores, Pero estas operaciones de control no se pueden usar indiscriminadamente en ninguna organización.

- La vigilancia de los trabajadores no está prohibida pero ha de adoptar límites muy claros. En este sentido, sólo puede efectuarse si los trabajadores interesados han sido previamente informados acerca de las intenciones del empleador, esto es, no cabe el control secreto del uso de internet, salvo que existan sospechas razonablemente justificadas de actividades delictivas u otras infracciones graves. En consecuencia, antes de que se pongan en marcha las actividades de vigilancia, los trabajadores deben conocer las finalidades de ésta y saber con precisión en qué períodos se efectuará.

- Es conveniente llegar a acuerdos, en el marco del convenio colectivo o del acuerdo de condiciones laborales, en las cuales se establezcan protocolos de actuación para el uso de internet por parte de los trabajadores y, en su caso, sobre los sistemas de control por parte de la entidad local. En cualquier caso, es mejor establecer la participación de los representantes sindicales en los procedimientos de control y es mejor prevenir, esto es, impedir el acceso a determinadas páginas electrónicas que sancionar por el acceso a las mismas.

Para ampliar información puede consultar los siguientes textos:

- OIT/96/29. Repertorio de recomendaciones prácticas sobre la protección de datos personales de los trabajadores.

143 ¿EN QUÉ CONDICIONES UN ORGANISMO PÚBLICO (UNA DIPUTACIÓN FORAL O EL GOBIERNO VASCO) PUEDE CEDER DATOS DE EXPEDIENTES DE LOS SERVICIOS SOCIALES A UN AYUNTAMIENTO SIN EL CONSENTIMIENTO PREVIO DE LA PERSONA TITULAR DE LOS DATOS?

- Según establece el artículo 11 de la LOPD, sólo pueden cederse los datos de expedientes de los servicios sociales entre las instituciones públicas citadas cuando se den una de las siguientes condiciones:
  - Que la cesión se produzca para cumplir fines directamente relacionados con las funciones legítimas del organismo cedente y del cesionario, y con el previo consentimiento de la persona interesada.
  - Cuando una ley regule expresamente la cesión.

- Debe establecerse un procedimiento que permita acreditar los siguientes hechos y competencias: la solicitud de los datos, la competencia de la entidad solicitante y la habilitación legal o el consentimiento del interesado para la cesión.

- Otra cuestión muy diferente es el derecho de los ciudadanos a no presentar documentos que ya se encuentren en poder de la administración actuante. En cualquier caso, este derecho no faculta a la administración a acceder a datos personales sin el requisito del consentimiento de su titular. Por el contrario, es el ciudadano el que ha de hacer valer su derecho, indicando qué documentos o datos son los que se encuentran ya en poder de la administración y cuya utilización autoriza, evitando así el tener que presentarlos de nuevo.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Arts. 42 a 44.
- Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las AAPP y del Procedimiento Administrativo Común: artículo 35 a).
- Real Decreto 1778/1994, de adecuación de la Ley 30/1992.

144 ¿PUEDE PROPORCIONARSE INFORMACIÓN DE UNA PERSONA MENOR O INCAPACITADA A SU PADRE O MADRE CUANDO LA GUARDA HA SIDO ASUMIDA POR LA DIPUTACIÓN FORAL? ¿Y A LAS PERSONAS QUE SE HACEN CARGO DEL MENOR EN UN PROGRAMA DE ACOGIMIENTO?

- Según el Código Civil, el ejercicio de la patria potestad es determinante para ostentar el ejercicio de la representación legal de menores o incapacitados. Como norma general, son los padres de los menores o incapacitados los que tienen la patria potestad atribuida y no la pierden salvo que incumplan sus deberes y el juez se la retire.

- Por tanto, en los dos supuestos planteados en la pregunta, el acceso a los datos relativos a los menores o incapacitados corresponde a los padres.

- Es importante diferenciar este supuesto de guarda del supuesto de asunción de tutela por parte de una entidad pública competente, ya que en este último caso sí se produce la suspensión de la patria potestad.

Para ampliar información puede consultar los siguientes textos:

- Código Civil: artículos 172.2 y 3.

145 ¿ES POSIBLE FACILITAR A LA PERSONA INTERESADA UNA COPIA DE LOS INFORMES O DICTÁMENES ELABORADOS POR DIFERENTES PROFESIONALES E INCLUIDOS EN EL EXPEDIENTE?

- Sí es posible. Según establecen la normativa general, la normativa de protección de datos y la normativa específica reguladora del acceso a archivos y documentos, cuando éstos contengan datos referidos a la intimidad de la persona, el acceso sólo podrá llevarse a cabo por la interesada. En consecuencia, la persona interesada tiene derecho a solicitar y obtener copia de todos los documentos que formen parte de su expediente.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 15.

146 ¿QUÉ FICHEROS DEBE DECLARAR UNA ENTIDAD LOCAL PRESTADORA DE SERVICIOS SOCIALES?

- Una entidad local debe declarar todos los ficheros que contengan datos de carácter personal, tanto si están informatizados como si están estructurados y en formato manual.

- A modo de ejemplo, en virtud de su rol prestador de servicios sociales, las entidades locales suelen declarar algunos de los siguientes ficheros:
  - Gestión de ayudas sociales.
  - Tramitación y gestión de recursos sociales.
  - Fichas sociales de personas atendidas y de intervenciones realizadas.
  - Solicitantes de asistencia social.
  - Usuarios de servicios sociales y de centros de atención social.
  - Ayudas de emergencia social.
  - Asistencia domiciliaria.
  - Discapacitadas.
  - Tratamiento de registros del servicio de tele alarma.
  - Beneficiarios del servicio de bienestar social.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 3.a.
- Consultar Registro de Protección de Datos en www.avpd.es.

147 ¿QUÉ DATOS TIENE QUE SOLICITAR UNA ENTIDAD LOCAL A UNA PERSONA PARA PRESTARLE UN SERVICIO SOCIAL?

- El principio de calidad de los datos de carácter personal establecido en la LOPD determina que sólo podrán recogerse y someterse a tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades para las que se hayan obtenido. Estas finalidades, a su vez, han de ser determinadas, explícitas y legítimas.

- En el ámbito de actuación de los servicios sociales generalmente es necesario recoger una gran cantidad de datos personales (económicos, formativos, sociofamiliares, laborales, psicológicos, etc.) para poder prestar la atención y ayuda adecuada a las necesidades de la persona.

- Como norma general, es necesario pedir el consentimiento previo de la persona antes de solicitar sus datos personales. Ahora bien, el acudir a los servicios sociales para requerir la prestación de un servicio supone un consentimiento inequívoco de la persona a la recogida de sus datos personales, siempre que los datos que se pretendan obtener puedan valorarse como adecuados, pertinentes y no excesivos con relación a la finalidad de asistencia psicosocial.

- En este sentido, es preciso evitar prácticas de solicitud de información personal que puedan suponer un entrometimiento en la esfera privada de la persona, al recabar datos irrelevantes, esto es, no adecuados, no pertinentes y excesivos.

- A la hora de determinar la recolección de datos personales mediante cuestionarios o entrevistas, incluso de datos delicados o especialmente protegidos, es necesario evaluar que la información personal que se va a solicitar tiene una relación directa, soportada por la literatura científica, con la decisión a tomar en materia de prestación social.

- Es difícil enumerar todos los tipos de datos que pueden manejarse con una finalidad de prestación social, pues su identificación dependerá de las características de la situación carencial o problemática que origine la petición o necesidad de ayuda. Parece más lógico enunciar reglas destinadas a garantizar la claridad de la operación y el conocimiento de la misma por la persona afectada.

- En todos los supuestos de datos especialmente protegidos, el tratamiento o uso de esos datos ha de realizarse respetando todos los principios que establece la LOPD, tales como del deber de secreto, el derecho a la información, etc.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art.4.

148 LOS DATOS PERSONALES RECOGIDOS CON LA FINALIDAD DE PRESTAR UN SERVICIO SOCIAL A LA TITULAR DE LOS DATOS, ¿PUEDEN UTILIZARSE PARA OTROS FINES DISTINTOS POSTERIORMENTE?

- No, los datos personales recogidos para el cumplimiento de una finalidad determinada, explícita y legítima, en este caso con el fin de prestar un servicio social, no pueden tratarse o utilizarse para otros fines que sean incompatibles con la finalidad de la recogida. Además, esta finalidad ha de ser conocida por la persona interesada con carácter previo a la recogida de sus datos.

- Sin embargo, no se considerará incompatible con la finalidad inicial declarada del acopio de datos personales, el tratamiento posterior de tales datos si se realiza con fines históricos, estadísticos o científicos.

- El tratamiento de datos personales cuyo propósito es el análisis y la investigación de carácter histórico, estadístico o científico con frecuencia puede llevarse a cabo con datos disociados, esto es, aplicando procedimientos de disociación a los datos personales cuyo acceso se facilita, de tal manera que se elimina la posibilidad de identificar a la persona titular de los datos.

- En otras ocasiones, tanto para fines de análisis histórico o científico como para conocer la realidad social y poder planificar las políticas públicas adecuadas a ella, es más relevante y útil emplear datos sociales o agregados, esto es, información referida a un grupo o colectivo social, en lugar de datos personales. En este sentido, la protección de los datos personales no es un obstáculo para que las entidades o los grupos sociales dispongan de la información necesaria que necesitan para realizar sus cometidos y evaluar los resultados de las políticas y programas públicos.

Para ampliar información puede consultar los siguientes textos:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 4.

149 ¿PUEDE UN EMPLEADO QUE TRABAJA EN LOS SERVICIOS SOCIALES DE UNA ENTIDAD LOCAL ACCEDER A LOS DATOS PERSONALES QUE EXISTEN EN LOS FICHEROS?

- Un empleado puede acceder exclusivamente a los datos personales que necesita para realizar las tareas que tiene encomendadas. En el documento de seguridad se especifica la relación de usuarios autorizados a acceder a los distintos ficheros de datos personales.

- Los ficheros de datos personales que se crean para prestar un servicio social suelen incluir datos especialmente protegidos, por ejemplo, datos de salud, de origen racial o derivados de actos de violencia de género. Por ello, requieren el establecimiento de un plus de medidas para garantizar la seguridad, que son clasificadas como medidas de nivel alto.

- Así, respecto a los ficheros automatizados hay medidas de seguridad especiales relacionadas con la identificación y distribución de soportes que contengan datos especialmente protegidos, con las copias de respaldo y recuperación y con el registro de accesos y de transmisión de estos datos a través de sistemas de telecomunicaciones.

- Es importante que recordemos las medidas a adoptar respecto de los ficheros no automatizados o manuales, debido a que todavía existen muchos ficheros de este tipo relacionados con la actividad de servicio social. En concreto:
  - Establecer mecanismos que permitan identificar a las personas que han accedido al fichero, cuando hay más de una persona con acceso autorizado.
  - Dotar de llaves, o de otros sistemas de control del acceso, a los locales donde se encuentran los expedientes.
  - Prohibir la posibilidad de realizar copias de los documentos de los expedientes a las personas no autorizadas.
  - Destruir las copias de los documentos que contienen datos personales mediante procedimientos que impidan su posterior recuperación.
  - Establecer la custodia obligatoria por parte de la persona autorizada de la documentación que no se encuentre en el archivo
  - Adoptar medidas que impidan el acceso de terceras personas cuando se trasladan físicamente los expedientes.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Arts. 24 al 40.
- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Arts. 7 a 9.
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Arts. 101 al 104 y 111 al 114.

ANEXO I

SUPUESTOS CONCRETOS

3. LA AGENCIA VASCA DE PROTECCIÓN DE DATOS, EL MANUAL DE BUENAS PRÁCTICAS Y EUDEL

150 ¿QUÉ ES LA AGENCIA VASCA DE PROTECCIÓN DE DATOS?

- Es una autoridad de control independiente, cuyas funciones son:
  - Vigilar que las administraciones públicas vascas, cuando manejan información sobre personas, cumplan la normativa de protección de datos personales. Para lograr este cometido realiza inspecciones, instruye expedientes y declara infracciones.
  - Atender las consultas y petición de informes que, en relación a la protección de datos, le solicitan las personas y las instituciones.
  - Potenciar la adopción de mejores prácticas en gestión de la información personal, por parte de los empleados públicos.
  - Informar y sensibilizar a la ciudadanía sobre su derecho a la privacidad y a la protección de sus datos personales.
  - Recoger en un Registro de Protección de Datos los tratamientos de datos personales realizados por las administraciones e instituciones de la Comunidad Autónoma del País Vasco (se inscriben los tipos de tratamiento de datos personales, pero no los datos personales).

Para ampliar información puede consultar los siguientes textos:

- Ley 2/2004, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

151 ¿CUÁLES SON LAS LÍNEAS DE COLABORACIÓN ENTRE LA AGENCIA VASCA DE PROTECCIÓN DE DATOS - AVPD Y LAS ENTIDADES LOCALES?

- La AVPD y la Asociación de Municipios Vascos - EUDEL han firmado un convenio de colaboración para promover el derecho a la protección de los datos personales en la gestión de la información municipal. Este Manual de Buenas Prácticas es resultado del trabajo colaborativo de ambas instituciones.

- La AVPD:
  - Ha mantenido reuniones presenciales con la mayoría de las entidades locales con el objeto de establecer un primer contacto, dar a conocer la misión y cometidos de la AVPD e informar a los alcaldes, concejales, secretarios y otros miembros de las entidades locales sobre los principios básicos, los derechos de la ciudadanía y las obligaciones legales de las organizaciones en materia de protección de datos.

- Ha planteado la creación de la figura de un/a coordinador/a de protección de datos en cada entidad local, para constituir una futura red de coordinadores en la materia, que permita el intercambio de información, de procedimientos, de prácticas y de propuestas de solución a las nuevas situaciones que surjan para una mejor gestión de la información personal.
- Da una primera respuesta a las necesidades y demandas formativas e informativas que presentan las entidades locales, a través de la edición de materiales de sensibilización, del diseño e impartición de acciones formativas y a través de la planificación de proyectos de cambio en gestión de datos personales.

152

¿QUÉ TAREAS LLEVA A CABO LA AVPD PARA CUMPLIR SU COMETIDO DE CONTROL DE LAS ENTIDADES LOCALES RESPECTO AL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS?

- La AVPD lleva a cabo las siguientes tareas de control:
  - Investigar actuaciones contrarias a la ley y **resolver sobre las infracciones** producidas, si las hubiera.
  - La AVPD inicia su labor de control de las administraciones públicas vascas a partir de la denuncia de una persona o, alternativamente, puede comenzar de oficio sus actividades de control cuando ha tenido conocimiento de posibles incumplimientos de la ley a través de los medios de comunicación, de otras administraciones o de terceras personas.
  - **Inspeccionar actuaciones por sectores de actividad pública**, para auditar o evaluar la gestión de datos personales que se realiza en un ámbito sectorial de actividad respecto al cumplimiento de la normativa legal y, en su caso, proponer recomendaciones y la adopción de buenas prácticas.

Para ampliar información puede consultar los siguientes textos:

- 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.

153

¿POR QUÉ SE REGISTRA COMO CÓDIGO TIPO EL MANUAL DE BUENAS PRÁCTICAS EN PROTECCIÓN DE DATOS PERSONALES PARA ENTIDADES LOCALES DE LA CAPV?

- Un Código Tipo en materia de protección de datos es un acuerdo o convenio administrativo o decisión de gestión que un sector de actividad privado (bancario, inmobiliario, de aseguramiento, etc.) o un sector público (hospitalario, escolar, de administración local, etc.) adopta para establecer las condiciones de organización, funcionamiento, procedimientos y normas para el tratamiento y uso de la información personal.

- La Asociación de Municipios Vascos - EUDEL, entre cuyos fines se encuentra la defensa y representación de los intereses generales de los municipios asociados, ha elaborado un Código Tipo en materia de protección de datos mediante la creación de un grupo de trabajo en el que han participado representantes de los ayuntamientos y de la AVPD. EUDEL establecerá un sistema para que las entidades locales se adhieran al código tipo y para comprobar el cumplimiento del mismo.

- La presentación del Código Tipo ante la AVPD y su inscripción en el Registro de Protección de Datos de Euskadi supone una garantía informativa para los ciudadanos que se relacionan con las entidades locales adheridas al mismo.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Arts. 57 a 62.

154 ¿QUÉ ES LA ASOCIACIÓN DE MUNICIPIOS VASCOS - EUDEL?

- La Asociación de Municipios Vascos, cuyas siglas son EUDEL - Euskal Udalaren Elkartea, es una entidad autónoma integrada por casi todos los municipios de la Comunidad Autónoma Vasca, varios municipios de la Comunidad Foral de Navarra y los municipios del Condado de Treviño.
- Se fundó en 1982 con el objetivo de defender la autonomía municipal y representar los intereses locales ante otras instituciones.
- EUDEL se ha convertido en un referente del municipalismo vasco y se erige en el principal interlocutor respecto a otras instituciones para la coordinación y consenso de las políticas públicas.
- Su reconocimiento en el derecho positivo se hace de manera singular en la legislación básica de Régimen Local.

Para ampliar información puede consultar los siguientes textos:

- Consulta página www.eudel.net.
- Consulta página www.eudel.net/aNG/web/cas/eudel/index.jsp.

155 ¿CÓMO SE FORMALIZA LA RELACIÓN DE COLABORACIÓN QUE MANTIENEN LA ASOCIACIÓN DE MUNICIPIOS VASCOS - EUDEL Y LA AGENCIA VASCA DE PROTECCIÓN DE DATOS - AVPD?

- EUDEL y la AVPD son dos entes independientes que han unido sus fuerzas para tratar de garantizar la protección de los datos personales en el ámbito de las administraciones locales.
- Para ello el 28 de septiembre de 2005 suscribieron un Convenio Marco de Colaboración donde se estipulan las relaciones entre ambas entidades.

Para ampliar información puede consultar los siguientes textos:

- Consulta página www.eudel.net/aNG/web/cas/docs/convenios/index.jsp. y www.avpd.es.
- Convenio Marco de Colaboración entre la Agencia Vasca de Protección de Datos y la Asociación de Municipios Vascos de 28 de septiembre de 2005.

156

¿CÓMO SE HA REALIZADO EL MANUAL DE BUENAS PRÁCTICAS EN MATERIA DE PROTECCIÓN DE DATOS PARA ENTIDADES LOCALES DE LA CAPV?

- Este Manual de Buenas Prácticas es uno de los resultados del Acuerdo Marco de Colaboración suscrito entre EUDEL y la AVPD el 28 de septiembre de 2005, por el que ambos entes se comprometían a realizar actuaciones tendentes a garantizar la protección de los datos personales en la administración local.

- Uno de los compromisos del Acuerdo Marco era el de crear una red de coordinadores de protección de datos dentro de las entidades locales vascas, para el diseño de procedimientos y herramientas útiles para la protección de datos de carácter personal, entre las que se encuentra este Manual de Buenas Prácticas.

- A partir de esta red de coordinadores de protección de datos pero de forma independiente, se ha creado una Comisión Técnica, formada por especialistas de diferentes ayuntamientos de la CAPV y por miembros de la AVPD y de EUDEL, que ha sido la que ha participado en la redacción del Manual de Buenas Prácticas.

157

EUDEL Y LOS DEPARTAMENTOS DE LAS DIPUTACIONES FORALES CON COMPETENCIAS EN ADMINISTRACIÓN LOCAL ¿CÓMO PROMOCIONAN EL DESARROLLO EN LAS ENTIDADES LOCALES DE BUENAS PRÁCTICAS EN GESTIÓN Y PROTECCIÓN DE DATOS PERSONALES?

- EUDEL y los departamentos forales de de las Diputaciones Forales de la CAPV con competencias en Administración Local han establecido las siguientes líneas de actuación para la promoción en las entidades locales de buenas prácticas en gestión y protección de datos personales:
  - Diseño de procedimientos, herramientas de trabajo y documentos tipo, bajo la dirección de la AVPD, para facilitar la adopción de buenas prácticas de protección de los datos personales que se manejan en las actividades municipales.

- Promoción de la adhesión de los ayuntamientos vascos al Manual de Buenas Prácticas en protección de datos de carácter personal, manual que tiene carácter de código tipo.
- Coordinación y Gestión, en colaboración con la AVPD, de actividades informativas y acciones formativas sobre gestión de la información y protección de datos personales.
- Distribución a las entidades locales vascas de los documentos, formularios, procedimientos, etc. que remita la AVPD para facilitar el cumplimiento de las obligaciones legales en materia de protección de datos de carácter personal.
- Encauzando las consultas de los Ayuntamientos Vascos sobre protección de datos a través de la AVPD en función de sus dictámenes.
- Instando a los Ayuntamientos Vascos a una permanente atención en la materia de protección de datos de carácter personal.

158 ¿QUÉ ES UN CÓDIGO TIPO PARA LA GESTIÓN Y PROTECCIÓN DE DATOS PERSONALES PARA ENTIDADES LOCALES DE LA CAPV?

- Los códigos tipo tienen por objeto adecuar lo establecido en la normativa de protección de datos personales a las peculiaridades de los tratamientos de datos personales efectuados por quienes se adhieren a los mismos. Para ello, contienen reglas o estándares específicos que permiten armonizar los tratamientos de datos efectuados por las entidades adheridas, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y el reglamento que la desarrolla.
- Los códigos tipo tienen el carácter de códigos deontológicos o de buena práctica profesional y son vinculantes para quienes se adhieran a los mismos.
- El Manual de Buenas Prácticas en protección de datos personales de las entidades locales tiene carácter de código tipo y pretende fomentar una mayor concienciación con relación al derecho a la privacidad y a la protección de datos en la gestión que llevan a cabo las personas que trabajan en las entidades locales.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales Art.56.
- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Art. 32.
- RD 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Arts. 71 al 78.

159 ¿CUÁL ES EL PROCEDIMIENTO DE ADHESIÓN AL MANUAL DE BUENAS PRÁCTICAS EN PROTECCIÓN DE DATOS PERSONALES?

- Cualquier entidad local de la CAPV puede adherirse al Manual de buenas prácticas, si realiza dos sencillas actuaciones:
  - Adoptar el acuerdo de adhesión al manual.
  - Comunicar a EUDEL que ha adoptado dicho acuerdo de adhesión al manual.

- Para utilizar los modelos de documentos y formularios que se incluyen en los anexos del manual, las entidades locales sólo tienen que introducir los distintivos gráficos de su institución o, en su caso, realizar modificaciones sencillas para adaptar los modelos a los estilos comunicativos propios de cada corporación.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Art. 58.

160 **¿CÓMO SE GESTIONA LA RELACIÓN DE ENTIDADES LOCALES ADHERIDAS AL MANUAL DE BUENAS PRÁCTICAS?**

- La Asociación de Municipios Vascos – EUDEL se encargará de actualizar la relación de entidades locales adheridas al manual y la comunicará o la pondrá a disposición de la Agencia Vasca de Protección de Datos – AVPD.
- Esta relación de entidades locales adheridas quedará incorporada al Manual de Buenas Prácticas como código tipo, en el Anexo VI, cuando transcurran seis meses desde su inscripción en el Registro de Protección de Datos de Euskadi.
- Esta relación de entidades locales adheridas al manual se podrá visualizar en el página web de EUDEL (www.eudel.net) y en la de la AVPD (www.avpd.es).

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Art.58.
- RD 1720 /2007, por el que se aprueba el Reglamento de la LOPD. Arts. 76 al 78.

161 **¿QUÉ OBLIGACIONES TIENE QUE CUMPLIR UNA ENTIDAD LOCAL SI SE ADHIERE A ESTE MANUAL DE BUENAS PRÁCTICAS EN PROTECCIÓN DE DATOS?**

- Las entidades locales que se adhieran a este Manual de Buenas Prácticas (MBP) están obligadas a:
  - Cumplir las normas establecidas en el MBP.

- Utilizar los modelos de documentos y formularios que se proponen en el MBP, con las adaptaciones al estilo gráfico o comunicativo de la corporación que resulten adecuadas.
- Establecer los procedimientos fijados en el MBP para que los ciudadanos puedan ejercitar los derechos denominados ARCO ante la entidad local.
- Aceptar el procedimiento de revisión del cumplimiento de lo dispuesto en el MBP y aceptar las sanciones que, en su caso, se establezcan por los incumplimientos.
- Planificar periódicamente actividades informativas y acciones formativas dirigidas a los empleados locales y, de manera preferente, a quienes traten datos sensibles o especialmente protegidos.
- Proporcionar a los trabajadores de la entidad un decálogo que sintetice los principios básicos de la protección de datos, los derechos de la ciudadanía y las obligaciones de las corporaciones municipales.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Arts. 2.2 y 60.

162

¿CÓMO SE EVALÚA SI UNA ENTIDAD LOCAL CUMPLE LO ESTIPULADO EN EL MANUAL DE BUENAS PRÁCTICAS?

- El Manual de Buenas Prácticas contempla que se establecerá un procedimiento de supervisión y un régimen sancionador como forma de control del cumplimiento de las obligaciones asumidas por las entidades locales adheridas.
- A estos efectos, se constituirá un grupo de trabajo de entre las entidades locales adheridas que, en los seis primeros meses de vigencia del Manual de Buenas Prácticas, ha de proponer la regulación de los procedimientos de supervisión y sanción.
- Los procedimientos de supervisión y sanción del cumplimiento del Manual de buenas prácticas que se aprueben se adjuntarán como anexos al Manual.
- La supervisión del cumplimiento del Manual y, en su caso, la propuesta de calificación de sanción por incumplimiento han de ser realizadas por personas con la suficiente cualificación y especialización técnica para hacerlo.

- En este sentido, una posibilidad de regulación de estos procedimientos es que sean realizados por los coordinadores de protección de datos y, para que este sistema de evaluación no tenga coste económico, aquellas entidades locales que se adhieran y que superen un determinado número de habitantes, podrían poner a su coordinador en protección de datos a disposición de otras entidades locales como experto evaluador del cumplimiento del manual.

Para ampliar información puede consultar los siguientes textos:

- MBP Entidades Locales. Art 59.