Guía básica de protección de datos para los entes locales

apdcat
Autoritat Catalana de Protecció de Dades

Generalitat de Catalunya

Edición

Autoridad Catalana de Protección de Datos

Primera edición: marzo 2012
Depósito legal: B-14703-2012

ÍNDICE

Presentación

El ejercicio de las funciones que tienen atribuidas los entes locales comporta que tengan que tratar un gran volumen de información de naturaleza diversa. Eso implica, necesariamente, el tratamiento de datos de carácter personal. Los entes locales no son los titulares de esta información, dado que los titulares son las personas físicas a las cuales se refiere, pero les corresponde custodiarla y tratarla de una forma diligente y con respeto a los derechos de las personas.

Con esta Guía se quiere ofrecer una primera aproximación a los principios, las garantías y las obligaciones que tienen que tener en cuenta los entes locales en su actuación, con el fin de ajustarla a lo que establece la normativa de protección de datos de carácter personal. Por eso, se han recogido los principios fundamentales y las obligaciones más relevantes, haciendo referencia tanto a la normativa aplicable en cada caso, como también a algunos ejemplos de las consultas que se nos han planteado con más frecuencia.

No se trata, por lo tanto, de un análisis exhaustivo de las cuestiones que se recogen, dado que el análisis más completo requerirá profundizar en la normativa aplicable, en la jurisprudencia recaída en esta materia y en los criterios y recomendaciones que ha ido formulando esta Autoridad. En este sentido, recordar que en la web de esta Autoridad (http://www.apd.cat) podréis encontrar tanto la normativa mencionada como las últimas resoluciones dictadas, como también los informes y los dictámenes emitidos.

Esperamos, pues, que sea una herramienta útil para desarrollar vuestra actividad y para conocer mejor el derecho fundamental a la protección de los datos de carácter personal.

Esther Mitjans Perelló
Directora de la Autoridad Catalana de Protección de Datos

Barcelona, febrero de 2012

1

MARCO NORMATIVO

El tratamiento de la información relativa a una persona física identificada o identificable requiere el cumplimiento de una serie de principios y obligaciones, establecidos en diferentes normas que hay que tener en cuenta

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas, ePrivacy), modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009.

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

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

- Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos.

- Decreto 48/2003, de 20 de febrero, por el cual se aprueba el Estatuto de la Agencia Catalana de Protección de Datos.

- Instrucción 1/2009, de 10 de febrero, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia.

También conviene tener en cuenta las siguientes recomendaciones publicadas:

- Recomendación 1/2008 de la Agencia Catalana de Protección de Datos, sobre la difusión de información que contenga datos de carácter personal a través de Internet.

- Recomendación 1/2010 de la Agencia Catalana de Protección de Datos, sobre el encargado del tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña.

- Recomendación 1/2011 de la Autoridad Catalana de Protección de Datos, sobre la creación, modificación y supresión de ficheros de datos de carácter personal de titularidad pública.

2

LEGITIMIDAD DEL TRATAMIENTO

Los entes locales pueden tratar los datos personales que resulten adecuados para el ejercicio de sus funciones

2.1 El principio de consentimiento

La LOPD reconoce y garantiza el derecho de las personas físicas a proteger su información personal. Las personas titulares de datos personales, como personas directamente afectadas o interesadas, tienen derecho a saber si un ente local dispone de estos datos, por qué motivo los tiene y para qué los quiere utilizar.

La información referida a personas físicas puede ser de diversos tipos (numérica, alfabética, gráfica, fotográfica, acústica) y puede referirse a un rasgo físico de la persona, a su situación económica o social, a sus estudios o a su profesión, a su salud, etc.

La información puede permitir identificar directamente a una persona (cuando disponemos del nombre y apellidos, de una fotografía, del DNI ...), o bien puede identificarla indirectamente (cuándo disponemos de una información que no está vinculada a una persona concreta, pero la asociamos con otros datos que sí que nos permiten identificarla sin esfuerzos desproporcionados).

La LOPD protege toda esta información, salvo los datos que no podamos relacionar con una persona concreta sin esfuerzos desproporcionados.

Tratar información personal quiere decir acceder a esta información (ya sea porque el mismo ciudadano la da al ente local o porque éste la recibe de terceras personas), como también almacenarla, modificarla, utilizarla, eliminarla o comunicarla a cualquier persona física o jurídica, ajena al ente, que no sea la misma persona interesada.

2.1.1 El consentimiento

El consentimiento es la pieza angular en la protección de datos. Constituye el principio sobre el cual se articula el poder de disposición y control de cualquier persona sobre sus datos. Así, cuando una entidad quiera desarrollar una actividad que requiera tratar datos de carácter personal, tiene que contar con el consentimiento de la persona afectada o, a falta de éste, con una ley que lo habilite.

Sin embargo, hace falta tener en cuenta que la misma LOPD habilita las **administraciones públicas**, y entre ellas los entes locales, para que recojan los datos necesarios para ejercer sus funciones, en el ámbito de sus competencias.

CONSENTIMIENTO

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

De acuerdo con la normativa de protección de datos, el consentimiento tiene que ser:

- **Inequívoco**: la solicitud y el otorgamiento del consentimiento se tienen que producir de forma clara.
- **Libre**: la persona tiene que disponer de la posibilidad de rechazar libremente que se traten sus datos.
- **Específico**: el consentimiento se refiere a tratamientos concretos y para una finalidad determinada, explícita y legítima del responsable del tratamiento, sin que se puedan hacer habilitaciones genéricas.
- **Informado**: hay que informar a las personas afectadas de acuerdo con lo establecido por el artículo 5 de la LOPD a fin de que, con antelación al tratamiento, puedan conocer de su existencia y finalidades.

El consentimiento se puede obtener de forma expresa o de forma tácita, a menos que se trate de datos especialmente protegidos, en que el consentimiento tiene que ser expreso.

Cuando sea admisible el consentimiento tácito, éste se puede obtener a través del mecanismo siguiente:

a) El responsable del tratamiento se puede dirigir a las personas afectadas, informarles en los términos del art. 5 LOPD y otorgarles un plazo de 30 días para manifestar su negativa al tratamiento.

b) Se tiene que ofrecer a la persona interesada un medio sencillo y gratuito para manifestar su negativa al tratamiento de sus datos en el plazo mencionado.

c) Si la persona interesada manifiesta su negativa, el responsable del fichero no puede volver a pedirle el consentimiento respecto del mismo tratamiento y las mismas finalidades, en el plazo de un año a contar desde la fecha de la solicitud anterior.

d) Si la persona interesada no se ha pronunciado al acabar el plazo, se entiende que consiente el tratamiento de los datos.

RESPONSABLE DEL FICHERO O DEL TRATAMIENTO	Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que sólo o conjuntamente con otros decide sobre la finalidad, el contenido y el uso del tratamiento, aunque no lo realice materialmente. También pueden ser responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

- ***¿Cómo se tiene que actuar en aquellos supuestos de pérdida de la documentación en la que se había recogido el consentimiento de la persona afectada para el tratamiento de sus datos de carácter personal?***

La entidad tiene que volver a pedir el consentimiento para el tratamiento o comunicación de datos de carácter personal, dado que le corresponde la carga de probar su otorgamiento.

Normativa aplicable: arts. 3. h), 5 y 6 LOPD; 5.1.d), 12 y 14 RLOPD.

2.1.2 Datos especialmente protegidos

El régimen general del consentimiento se refuerza en el caso del tratamiento de datos especialmente protegidos o sensibles. Hay que diferenciar los supuestos siguientes:

a) Datos que revelan la **ideología, la afiliación sindical, la religión y las creencias**: sólo se pueden tratar con el consentimiento expreso y por escrito, con la advertencia a la persona interesada respecto de su derecho a no facilitar estos datos.

b) Datos que se refieren al **origen racial**, la **salud** y la **vida sexual**: sólo se pueden tratar cuando, por razones de interés general, así lo disponga una ley o la persona afectada consienta expresamente.

c) Datos relativos a la **comisión de infracciones penales y administrativas:** la creación de ficheros para recopilar estos datos sólo lo pueden llevar a cabo las administraciones públicas competentes, de acuerdo con las normas reguladoras respectivas.

No obstante, excepcionalmente, los datos especialmente protegidos se pueden tratar, sin consentimiento, cuando sea necesario para la prevención o el diagnóstico médicos, la prestación de asistencia sanitaria o de tratamientos médicos, la gestión de servicios sanitarios, por parte de profesionales sanitarios u otras personas sujetas al secreto profesional, o para la salvaguarda del interés vital de la persona afectada o de otra persona, en caso de que la persona afectada esté físicamente o jurídicamente incapacitada para dar su consentimiento.

- ***¿Se pueden comunicar datos que forman parte de la historia clínica de un paciente a un familiar sin su consentimiento?***

  Según la Ley 21/2000, el acceso al historial clínico tan sólo lo puede pedir el paciente o su representante debidamente acreditado, dado que se trata de un derecho personalísimo. Sólo se tiene que informar a las personas vinculadas al paciente en la medida en que éste lo permita expresamente o tácitamente.

  En caso de incapacidad del paciente, éste tiene que ser informado de acuerdo con su grado de comprensión, sin perjuicio de tener que informar también a quien ostenta su representación.

  Si el paciente, a criterio del médico responsable de la asistencia, no es competente para entender la información, porque se encuentra en un estado físico o psíquico que no le permite hacerse cargo de su situación, se tiene que informar también a los familiares o las personas que están vinculadas al paciente.

- ***¿Puede una cámara de videovigilancia registrar imágenes que contengan datos especialmente protegidos, sin el consentimiento de las personas afectadas y sin una habilitación legal?***

No, excepto las captaciones de imágenes de las personas en que, de forma meramente accesoria, se puedan tratar rasgos físicos, la apariencia, hábitos o comportamientos.

Normativa aplicable: arts. 7 y 8 LOPD; 3, 6 y 7 Ley 21/2000; 5.2 Instrucción 1/2009.

2.1.3 Datos recogidos por las policías locales

En relación con los datos de carácter personal recogidos y tratados por las policías locales y el resto de Fuerzas y Cuerpos de Seguridad con finalidades policiales, **no hace falta el consentimiento** de la persona afectada en los supuestos y respecto de las categorías de datos que sean necesarios para prevenir un peligro real para la seguridad pública o para la represión de infracciones penales.

Respecto de los datos **especialmente protegidos**, las Fuerzas y Cuerpos de Seguridad los pueden recoger y tratar exclusivamente en los supuestos en que sea absolutamente necesario para una investigación concreta.

- ✓ Estos datos se tienen que **almacenar** en ficheros específicos establecidos a este efecto, que se tienen que clasificar por categorías de acuerdo con su grado de fiabilidad. Así, no se puede otorgar el mismo grado de fiabilidad a meras sospechas no contrastadas, que a informaciones relativas a una determinada imputación o sobre una persona que ha sido condenada o absuelta.

- ✓ Se tienen que **cancelar** cuando ya no sean necesarios para la finalidad para la cual se recogieron.

- ✓ En aquellos casos en que se pueda producir un peligro para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que estén abiertas, se puede **denegar** el acceso, la rectificación o la cancelación de los datos.

- ***¿Las policías locales de Cataluña pueden acceder a las grabaciones de las cámaras de videovigilancia de una entidad?***

  Si es en el curso de una investigación, la ley prevé que la policía pueda acceder a las grabaciones.

Normativa aplicable: arts. 22 LOPD; 9 LOVFCS; 9 Decreto 78/2010; 15 Decreto 134/1999; 1 Orden de 29 de junio de 2001; 5.1 y 18 Instrucción 1/2009.

2.1.4 Datos relativos a menores de edad

En caso de tratar datos de menores de edad, hay que tener en cuenta:

- Si son **mayores de catorce años,** es suficiente con su consentimiento, salvo los casos en que la ley exija la asistencia de las personas titulares de la patria potestad.

- Si son **menores de catorce años**, siempre es necesario el consentimiento de los padres o tutores.

No se pueden obtener a través de un menor datos que permitan obtener información sobre el resto de miembros del grupo familiar o sus características (actividad profesional de los progenitores, información económica…), sin consentimiento de las otras personas afectadas, a menos que se trate de los datos referentes a la identidad y la dirección de los progenitores con el fin de poder obtener su consentimiento.

La protección de los menores se concreta también en la exigencia que la información que se les proporciona sea en un lenguaje fácilmente comprensible para ellos.

- ***¿Puede un casal de verano municipal recoger el dato relativo a las direcciones de los correos electrónicos de los padres, a través de los menores de edad que son inscritos, con el fin de ponerse en contacto con ellos?***

  Como norma general, hay que contar con el consentimiento de los padres para recoger el dato relativo a su correo electrónico. Excepcionalmente, puede facilitarlo directamente el menor, en los casos en que sea necesario completar la capacidad del menor de edad a través de sus progenitores, a fin de que éstos puedan consentir el tratamiento de los datos del menor.

Normativa aplicable: art. 13 RLOPD.

2.1.5 Revocación del consentimiento

El consentimiento otorgado por la persona afectada se puede **revocar** en cualquier momento, sin efectos retroactivos, siempre que haya una causa justificada:

- El responsable del fichero tiene que establecer un medio sencillo a través del cual la persona interesada pueda revocar el consentimiento. El responsable del fichero dispone de un plazo de 10 días, desde que recibe la solicitud, para cesar en el tratamiento y, si procede, para cancelar los datos.

- La persona interesada puede solicitar al responsable del tratamiento la confirmación del cese. Esta solicitud se tiene que responder expresamente.

- Si el responsable del tratamiento, con carácter previo a la revocación del consentimiento, ha cedido datos a uno tercero, tiene que comunicarle la revocación del consentimiento dentro del mismo plazo de 10 días, a fin de que también cese en el tratamiento y, si procede, cancele los datos.

Normativa aplicable: arts. 6 LOPD; 12 y ss. RLOPD.

2.1.6 Tratamiento en supuestos de falta de consentimiento

A pesar de lo que acabamos de exponer, hay una serie de supuestos regulados en la LOPD en **los cuales no es necesario el consentimiento** de la persona afectada, concretamente cuando:

- Así lo establezca una norma con rango de ley.
- Se recojan para el ejercicio de funciones propias de las **administraciones públicas,** en el ámbito de sus competencias.
- Se refieran a las partes de un contrato o precontrato de una relación laboral, negocial o administrativa y sean necesarios para mantenerla o cumplirla.
- El tratamiento de los datos tenga como finalidad proteger un interés vital de la persona interesada.
- Los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para satisfacer el interés legítimo perseguido por el responsable del fichero o por el tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales de la persona interesada.

FUENTES ACCESIBLES AL PÚBLICO	Ficheros que puede consultar cualquier persona, sin que lo impida una norma limitativa o sin otra exigencia, que el abono de una contraprestación, si procede. Sólo se consideran fuentes de acceso público el censo promocional, los diarios y los boletines oficiales, los medios de comunicación, las guías de servicios de comunicaciones electrónicas, en los términos que prevé la normativa específica, y las listas de personas que pertenecen a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo.

- ***¿Se requiere el consentimiento de las personas afectadas para que el ayuntamiento pueda tratar los datos en un expediente iniciado de oficio? ¿Y si el procedimiento se ha iniciado a instancia de parte?***

  No es necesario el consentimiento de la persona afectada en aquellos tratamientos de datos de carácter personal que estén relacionados con las funciones propias de las administraciones públicas, en el ámbito de sus competencias. Por lo tanto siempre que esta información se obtenga en relación con el desarrollo de sus competencias, no hace falta su consentimiento.

- ***¿La incorporación de datos al padrón municipal requiere el consentimiento de las personas afectadas?***

  Los datos del padrón constituyen prueba de la residencia y el domicilio habitual en el municipio.

  Existe la obligación de facilitar estos datos, hecho que supone una excepción legal al principio del consentimiento. Esta obligación siempre tiene que estar vinculada con la finalidad del padrón.

- ***¿Hay que pedir el consentimiento de los trabajadores de un ente local para tratar sus datos por medio de la lectura de la huella dactilar, con la finalidad de control horario?***

  No, en la medida en que la recogida de datos personales de los trabajadores públicos se realice dentro de una relación jurídica laboral o administrativa y tenga como finalidad el control, precisamente, de su cumplimiento.

- ***¿Puede una empresa municipal tratar datos de carácter personal recogidos de otras webs (números de teléfono, direcciones electrónicas personales, nombres y apellidos…)?***

  No, a menos que se cuente con el consentimiento de las personas afectadas. El hecho de que los datos se encuentren accesibles en una web no las convierte en fuentes accesibles al público.

Normativa aplicable: arts. 3.j), 6.2 LOPD; 7, 10.3 y 12.1 RLOPD.

2.2 El principio de calidad de los datos

Es el segundo de los principios primordiales con respecto al derecho fundamental a la protección de datos. En realidad se trata de un principio que se desgrana en diversos principios que se regulan en la LOPD y en el RLOPD.

2.2.1 Principio de proporcionalidad

Sólo se pueden tratar los datos que sean **adecuados**, **pertinentes** y **no excesivos** en relación con la finalidad del tratamiento.

2.2.2 Principio de finalidad

Los datos se tienen que destinar a la finalidad determinada, explícita y legítima para la cual se recogieron. Es contrario a este principio cualquier uso que se haga destinado a una finalidad incompatible con aquélla para la cual se hayan recogido. No es incompatible el tratamiento con finalidades históricas, estadísticas o científicas.

2.2.3 Principio de exactitud

Los datos tienen que ser exactos y puestos al día, con el fin de reflejar la situación real de las personas afectadas. Cuando los datos sean inexactos se deben rectificar, no sólo a petición de la persona afectada en ejercicio de su **derecho de rectificación**, sino también de oficio, en el mismo momento en que la entidad responsable del tratamiento tenga conocimiento de la inexactitud.

- ✓ Si los datos son o se convierten en inexactos, en todo o en parte, o incompletos, se tienen que **rectificar de oficio**.

- ✓ Si los datos ya no son necesarios o pertinentes de acuerdo con la finalidad para la cual se recogieron o registraron, se tienen que **cancelar**.

2.2.4 Conservación

Los datos se tienen que cancelar cuando dejen de ser necesarios o pertinentes. Sólo se pueden conservar durante un periodo superior al necesario para la finalidad para la cual se recogieron si se anonimizan o se disocia la información que contienen, o si se quieren conservar, con la autorización de la Autoridad Catalana de Protección de Datos, considerando los valores históricos, estadísticos o científicos de acuerdo con la legislación específica.

No obstante, los datos cancelados se tienen que conservar, a disposición de las administraciones públicas, jueces y tribunales, debidamente bloqueados durante el transcurso del tiempo en que se pueda exigir algún tipo de responsabilidad derivada de una relación u obligación jurídica, de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por la persona afectada. Transcurrido este plazo, se tienen que suprimir.

Ahora bien, si los datos se han obtenido por medios fraudulentos, desleales o ilícitos, se tienen que destruir directamente.

Para determinar el periodo de conservación de los documentos hay que tener en cuenta las previsiones sobre evaluación documental contenidas en la normativa de archivos.

- ***¿Se cumple con la obligación de cancelar los datos si la información personal se anonimiza o disocia de forma irreversible?***

  La anonimización o disociación de un dato, de manera que no se pueda identificar el titular, cumple esta obligación de cancelación.

- ***¿Durante cuánto tiempo se pueden conservar las imágenes obtenidas a través de un sistema de videovigilancia?***

  En los supuestos en que no se pueda alcanzar la finalidad perseguida sin almacenar las imágenes, el periodo de conservación no tiene que ser superior al que resulte necesario para el cumplimiento de la finalidad de vigilancia para la cual se han recogido o registrado.

  Con carácter general, se recomienda no exceder el plazo máximo de un mes para cancelar las imágenes.

2.2.5 Principio de lealtad

Cualquier entidad que trate datos personales lo tiene que hacer de manera leal, lícita y sin utilizar medios fraudulentos.

Normativa aplicable: arts. 3.f) y 4 LOPD; 9 LA; 5.1.e), 5.1.p), 8 y 157-158 RLOPD; 6, 7 y 8 Instrucción 1/2009; art. 10.2 LUMESPC.

3

OBLIGACIONES PREVIAS AL TRATAMIENTO

Antes de iniciar la recogida de los datos, hace falta disponer del fichero correspondiente, notificarlo a la Autoridad Catalana de Protección de Datos e informar a las personas afectadas

La implementación de la normativa de protección de datos exige a las entidades la definición de un plan de adecuación, que permita conocer cuál es la situación de todos los ficheros y tratamientos de datos personales que se realizan dentro de la entidad y el análisis de cómo están interconectados. Se tiene que analizar el "ciclo de vida" o recorrido de los datos a lo largo de su tratamiento, con el fin de identificar:

- Qué datos personales se tienen que recoger y para qué finalidad.
- Cómo se recogerán (formularios, electrónicamente, telefónicamente...).
- Qué ficheros hay que crear y, si procede, qué ficheros hace falta modificar o suprimir.
- Quién los tratará (áreas, departamentos, personas usuarias ...).
- Cómo circularán dentro de la entidad (en soporte papel, telemáticamente...).
- A quién se cederán o qué transferencies internacionales se llevarán a cabo
- Cómo se conservarán i, si procede, cómo y cuándo se destruirán.

3.1 La creación, la modificación y la supresión de los ficheros

Cuando el ejercicio de las funciones propias de un ente local comporte la recogida y el tratamiento posterior de datos de carácter personal, independientemente que el tratamiento se tenga que realizar de forma automatizada o no, hay que **crear** uno o diversos ficheros con carácter previo al inicio del tratamiento.

FICHERO Cualquier conjunto organizado de datos de carácter personal que permita el acceso a los datos de acuerdo con criterios determinados, sea cuál sea la forma o la modalidad de creación, almacenaje, organización y acceso.

Con el paso del tiempo, es posible que determinadas circunstancias obliguen a **modificar** el contenido de los ficheros. Puede ser necesario modificar un fichero porque cambia el responsable, o porque se amplían los usos, o porque hay que hacer un tratamiento de datos que no se había previsto inicialmente y que puede comportar, además, un cambio en el nivel de medidas de seguridad aplicable al fichero. Cualquier cambio que afecte, sustancialmente, al tratamiento de datos configurado inicialmente con la creación del fichero hace necesaria la modificación de este fichero.

Finalmente, es posible que determinados ficheros se tengan que **suprimir**. Por ejemplo, porque el ente local deja de prestar un servicio determinado y, en consecuencia, ya no es pertinente tratar determinados datos personales, o porque los datos que se trataban en un fichero pasan a formar parte de otro fichero, dentro del mismo ente local. En este caso, hace falta prever el destino que tendrán los datos y valorar si se tiene que derogar la disposición o acuerdo de creación correspondiente, que haya podido quedar sin contenido.

Según cuál sea la naturaleza, pública o privada, de la entidad responsable del fichero, los ficheros pueden ser de titularidad pública (entes locales, consorcios, organismos autónomos locales, etc.) o privada (sociedades privadas municipales, fundaciones, etc.).

- ***¿Quién es el responsable de los ficheros en el seno de un ente local?***

  Normalmente es el órgano administrativo que trate la información y tenga competencias en la materia y que tenga capacidad de decidir sobre el contenido, la finalidad y el uso del tratamiento de datos que se realice. Estará determinado por la ordenanza municipal o por la disposición que lo cree.

Normativa aplicable: arts. 3.d), 20 y 25, 44.3.a) LOPD; 5.1.m), n) y q), 52 y ss. RLOPD; 9 Instrucción 1/2009; Recomendación 1/2011.

3.1.1 Ficheros de titularidad pública

FICHERO DE TITULARIDAD PÚBLICA	Ficheros los responsables de los cuales sean órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a estos órganos, las administraciones públicas territoriales, así como las entidades u organismos que están vinculados o dependen de ellos y las corporaciones de derecho público, siempre que, en este último caso, estén vinculados al ejercicio de las potestades de derecho público que les atribuye su normativa específica.

Los ficheros de titularidad pública se tienen que crear, modificar o suprimir mediante una **disposición de carácter general**, es decir, una disposición dictada en ejercicio de la potestad normativa que corresponde a los entes locales. Esta disposición se tiene que aprobar y publicar con carácter previo al inicio del tratamiento de los datos.

Instrumento de aprobación:

- En el caso de los entes locales y los entes públicos vinculados o que dependen de ellos, los ficheros se pueden aprobar por **ordenanza o reglamento del pleno de la corporación**. En el caso del ayuntamiento de Barcelona también se pueden aprobar, de acuerdo con su régimen especial, por decreto de la Alcaldía o de la Junta de Gobierno Local.

- Si se trata de los ficheros de un Grupo municipal, se pueden aprobar por acuerdo del Grupo.

- Cuando se trate de consorcios:

  - ✓ Si dependen de un determinado ente local, se pueden aprobar por ordenanza o reglamento del ente local.
  - ✓ Si la representación de la Generalitat en sus órganos de gobierno es mayoritaria, se pueden aprobar mediante orden del consejero correspondiente o decreto del Gobierno de la Generalitat.
  - ✓ Si no hay una relación de dependencia respecto de ningún ente local determinado, ni de la Generalitat, se pueden aprobar por acuerdo del órgano superior del consorcio.

Contenido:

Los artículos 20 de la LOPD y 54 del RLOPD exigen que la disposición general o acuerdo de **creación** de nuevos ficheros haga referencia a:

a) La denominación del fichero o tratamiento.

b) La finalidad y los usos previstos.

c) Las personas o los colectivos afectados.

d) El procedimiento de recogida de los datos personales.

e) La procedencia de los datos personales.

f) La estructura del fichero:

- Tipología de los datos, con descripción detallada de los datos identificativos y, si procede, de los datos especialmente protegidos, y de las restantes categorías de datos.

- El sistema de tratamiento utilizado en su organización.

g) Las cesiones de datos personales previstas.

h) Las transferencias internacionales de datos personales previstas con indicación, si procede, de los países de destino de los datos.

i) El órgano o los órganos responsables del fichero.

j) Los servicios o las unidades ante las cuales se pueden ejercer los derechos de acceso, rectificación, cancelación y oposición.

k) El nivel de seguridad exigible.

Durante la fase de elaboración de la disposición, los entes locales pueden solicitar un informe potestativo a la Autoridad Catalana de Protección de Datos. Se recomienda adjuntar, a la solicitud del informe, una copia de la memoria del expediente. En caso de que se creen ficheros de videovigilancia, la memoria tiene que incluir la información requerida en el artículo 10 de la Instrucción 1/2009.

Con respecto a la disposición o el acuerdo de **modificación** del fichero, se tiene que indicar en cada caso cuáles de los anteriores apartados se ven afectados por la modificación. Se recomienda reproducir, a continuación, nuevamente el fichero entero con las modificaciones incorporadas, con el fin de facilitar la consulta a cualquier persona interesada.

La disposición o el acuerdo de **supresión** debe establecer el destino de los datos o, en su caso, las previsiones que se adopten para destruirlos.

Las disposiciones o acuerdos de creación, de modificación y de supresión de ficheros se tienen que publicar en el BOP, y también se debe incluir una referencia en el DOGC.

En relación con la creación, la modificación y la supresión de ficheros, consultad también la Recomendación 1/2011, de la Autoridad Catalana de Protección de Datos sobre la creación, modificación y supresión de ficheros de datos de carácter personal de titularidad pública.

- ***¿Se puede añadir una nueva finalidad a un fichero existente?***

  Sí, pero sólo si se trata de una finalidad compatible con la que ya tenía el fichero. En cualquier caso hay que modificar el fichero y, si procede, informar a las personas afectadas.

Normativa aplicable: arts. 20.1, 20.3 y 25 LOPD; 49 LRBRL; 39 Ley 13/2008; 5.n) y D.F 3ª LACPD; 26 y 27 Ley 22/98; 61 y ss. Ley 26/2010; 60 y ss. ROAS; 52 y ss. RLOPD; 178 TRLMRLC; 9 y 10 Instrucción 1/2009; Recomendación 1/2011.

3.1.2 Ficheros de titularidad privada

FICHERO DE TITULARIDAD PRIVADA	Ficheros los responsables de los cuales sean personas, empresas o entidades de derecho privado, con independencia de quien tenga la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros los responsables de los cuales sean corporaciones de derecho público no vinculados al ejercicio de las potestades de derecho público que les atribuye su normativa específica.

En la **creación** de ficheros de titularidad privada, como el caso de las sociedades municipales u otros entes dependientes que sean de derecho privado, hay libertad de forma. A diferencia de los ficheros de titularidad pública, no se requiere la aprobación de ninguna disposición. Es suficiente con la voluntad del responsable del fichero (es decir, la decisión conforme se quieren crear unos ficheros destinados a una finalidad concreta, cuando sea necesario para alcanzar la actividad o el objeto legítimo de la entidad titular), y la notificación al Registro de Protección de Datos de Cataluña.

- ***¿Se puede incluir un fichero de titularidad privada dentro de una disposición de creación de ficheros de titularidad pública?***

  Sí, es posible. Sin embargo, ello no alterará su naturaleza privada y condicionará su futura modificación y supresión, dado que también se tendrá que hacer mediante una disposición general.

Normativa aplicable: arts. 25 LOPD; 5.1.l), 55 y ss. RLOPD.

3.2 La notificación de los ficheros o tratamientos

La creación o, si procede, la modificación o la supresión de los ficheros se tiene que **notificar** al Registro de Protección de Datos de Cataluña de la Autoridad Catalana de Protección de Datos. Una vez inscritos, la Autoridad da traslado al Registro General de Protección de Datos de la Agencia Española de Protección de Datos.

- ✓ El plazo para presentar las solicitudes de inscripción es de 30 días desde su publicación.

- ✓ Los ficheros se **inscribirán** una vez verificado el cumplimiento de los requisitos legalmente establecidos en la LOPD y en el RLOPD.

- ✓ Transcurrido un mes desde la presentación de la solicitud de inscripción, sin que se haya resuelto, se entenderá inscrito el fichero a todos los efectos.

La inscripción de los ficheros tiene que estar permanentemente **actualizada**. Cualquier modificación que afecte a su contenido se tiene que notificar a la Autoridad Catalana de Protección de Datos.

- ***¿A quién corresponde notificar la creación, la modificación o la supresión del fichero?***

  Al responsable del fichero.

- ***¿A qué registro tiene que notificar sus ficheros una empresa privada que disponga de una concesión pública?***

  Siempre que los ficheros estén directamente vinculados a la prestación del servicio objeto de la concesión, se encontrarán dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos y, por lo tanto, se tienen que notificar al Registro de Protección de Datos de Cataluña.

- ***¿Dónde se tiene que hacer la notificación en caso de que se quieran modificar o suprimir unos ficheros previamente inscritos en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos, pero que ahora se encuentren dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos?***

  Tanto las modificaciones como las supresiones de los ficheros inscritos en el Registro General de Protección de Datos que se encuentren dentro del ámbito de actuación de la Autoridad Catalana de Protección de Datos se tienen que tramitar ante el Registro de Protección de Datos de Cataluña.

Normativa aplicable: arts. 26 LOPD; 5.i) LACPD; 55 y ss, 130 y 131 RLOPD; 11 Instrucción 1/2009; Recomendación 1/2011; Res. APDCAT 04.04.2011.

3.3 La información a la persona titular de los datos

Para poder iniciar el procedimiento de recogida de los datos, y con independencia que sea necesario el consentimiento o se cuente con habilitación legal, el responsable del tratamiento tiene que garantizar el derecho de información a cada una de las personas afectadas. Su omisión puede comportar un vicio del consentimiento.

Corresponde al responsable del fichero o tratamiento poder acreditar el cumplimiento de esta obligación.

Las personas titulares de los datos tienen que ser informadas previamente de forma **expresa**, **precisa** e **inequívoca** sobre:

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

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

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

d) La posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.

e) La identidad y la dirección del responsable del tratamiento o, si procede, de su representante.

(No es necesario dar la información de los apartados b), c) y d) si se deduce claramente de la naturaleza de los datos o de las circunstancias concurrentes)

Cuando se utilicen formularios o impresos para recoger los datos, éstos tienen que incorporar, de forma clara y legible, las advertencias anteriores, con independencia que sea o no necesario recoger el consentimiento.

También se puede dar cumplimiento a este deber de otras maneras, como por ejemplo, mensajes pregrabados, comunicaciones por escrito, carteles, etc. que sean aptos para que el ciudadano tenga pleno conocimiento de esta información, de acuerdo con el medio utilizado para la recogida.

Si los datos no se recogen directamente de su titular, sino que los cede o comunica una tercera persona, se le tiene que informar, dentro de los tres meses siguientes al momento de recibir los datos, de manera **expresa**, **precisa** e **inequívoca** sobre:

a) El contenido del tratamiento.

b) La procedencia de los datos.

c) La existencia de un fichero o un tratamiento de datos de carácter personal, de la finalidad de la recogida de los datos y de los destinatarios de la información.

d) La posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.

e) La identidad y la dirección del responsable del tratamiento o, si procede, de su representante.

(La información de los apartados c), d) y e) sólo se tiene que facilitar si no se ha informado la persona titular anteriormente)

Excepciones al deber de información:

- Cuando el cumplimiento del deber de información afecte a la defensa nacional, la seguridad pública o la persecución de infracciones penales, no es obligatorio el cumplimiento del deber de información.

- Si los datos no se recogen directamente de su titular, en los supuestos siguientes:

    a) Cuando una ley prevea expresamente la comunicación.

    b) Cuando el titular ya haya sido informado con anterioridad.

    c) Cuando el tratamiento tenga finalidades históricas, estadísticas o científicas.

    d) Cuando resulte imposible o exija esfuerzos desproporcionados, con autorización de la Autoridad Catalana de Protección de Datos.

    e) Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial.

- ***¿Cuando no es necesario el consentimiento, hay que informar igualmente?***

  Sí. El deber de información se tiene que cumplir en todos los casos, a menos que concurra alguna de las excepciones descritas.

- ***¿Qué medidas se requieren para cumplir con el deber de información, en los supuestos de sistemas de videovigilancia?***

  Las personas responsables del tratamiento de imágenes a través de cámaras fijas tienen que informar de forma clara y permanente sobre la existencia de las cámaras, aunque las imágenes no se registren, mediante la colocación de los carteles informativos que sean necesarios para garantizar su conocimiento, de acuerdo con los requisitos del artículo 12 de la Instrucción 1/2009.

Normativa aplicable: arts. 5, 24 LOPD; 5.p) LACPD; 13.3 RLOPD; 12 Instrucción 1/2009.

4

OBLIGACIONES DURANTE EL TRATAMIENTO DE LOS DATOS

Los principios y las obligaciones y las garantías previstas por la normativa de protección de datos se deben tener en cuenta no sólo en el momento de la recogida de los datos, sino también durante cualquier fase del tratamiento

La persona afectada dispone de una serie de garantías encaminadas a asegurar la adecuación del tratamiento de sus datos personales a la normativa vigente, que son de aplicación durante la recogida, el almacenaje, la utilización o la comunicación de los datos de carácter personal e incluso después de que finalice la relación jurídica. Estas garantías son:

- El deber de secreto.
- Los derechos de acceso, rectificación, cancelación y oposición.
- La implementación de medidas de seguridad.

4.1 El deber de secreto

El responsable del fichero y todas las personas que intervengan en cualquiera de las fases del tratamiento de datos de carácter personal están obligadas a guardar secreto profesional respecto de estos datos.

Esta obligación subsiste incluso después de la finalización de sus relaciones con el responsable.

Con el fin de garantizar el cumplimiento de este deber, es recomendable incorporar y definir esta obligación en los contratos laborales, en los protocolos internos y en las regulaciones específicas que recogen los derechos y las obligaciones de las partes en una relación jurídica que comporte el tratamiento de datos de carácter personal.

Normativa aplicable: arts. 10 LOPD; 83 y 123 RLOPD; 164.6 TRLMRLC.

4.2. La comunicación de datos personales

A pesar de la vigencia del deber de secreto, hay determinados supuestos en que el ejercicio de las competencias del ente local o de otras administraciones o entidades públicas puede comportar la necesidad de comunicar determinados datos a terceras personas o entidades. En estos casos, hay que sujetarse al régimen de cesiones o comunicaciones previsto en la LOPD.

CESIÓN O COMUNICACIÓN DE DATOS PERSONALES	Toda revelación de datos personales hecha a una persona diferente a la persona afectada.

4.2.1 Requisitos:

Para que una cesión o comunicación sea legítima, tiene que cumplir **con dos requisitos**:

- Que responda al cumplimiento de las **finalidades** directamente relacionadas con las funciones legítimas del cedente y del cesionario.

- Que se haya obtenido el **previo consentimiento** de la persona afectada o que concurra alguna de las circunstancias siguientes:

    a) Esté autorizada por una ley.

    b) Se trate de datos recogidos de fuentes accesibles al público.

    c) Responda a la libre y legítima aceptación de una relación jurídica que implique necesariamente la comunicación.

    d) El destinatario sea el Defensor del Pueblo, el Ministerio Fiscal y los jueces o tribunales o los tribunales de cuentas y las instituciones autonómicas análogas, en el ejercicio de sus funciones.

    e) En datos relativos a la salud, en casos de urgencia o para elaborar estudios epidemiológicos.

La comunicación de datos **entre administraciones públicas** está específicamente regulada en la LOPD, que prevé la posibilidad de ceder datos a otra administración pública sin disponer del consentimiento de las personas afectadas cuando:

- Se comuniquen para el ejercicio de las mismas competencias.

- Se comuniquen para el ejercicio de competencias que versen sobre la misma materia.

- La comunicación tenga por objeto el tratamiento de los datos con finalidades históricas, científicas o estadísticas.

- Una administración pública las obtenga o elabore con destino a otra administración.

- ***¿Se pueden ceder datos del padrón municipal a personas físicas o jurídicas de naturaleza privada diferentes de la persona afectada?***

  Puesto que las personas físicas o jurídicas de naturaleza privada no son administraciones públicas, no procede cederlos, dado que resulta contrario a las previsiones de la LOPD, la LRBRL y el TRLMRLC, a menos que se cuente con el consentimiento de las personas afectadas o de algún supuesto previsto en la legislación vigente.

- ***¿Puede un ayuntamiento comunicar individualmente a sus ciudadanos los datos que constan en el padrón municipal de habitantes, a través de consultas telefónicas?***

Sí, cuando se trate de la persona titular de los datos, siempre que se establezcan mecanismos para asegurar que la persona que solicita la información realmente lo sea.

- ***¿Se pueden utilizar los datos del padrón municipal para proponer a todos los vecinos la posibilidad de inscribirse en un nuevo registro del ayuntamiento, para poder recibir información de carácter municipal?***

Sí, es posible acceder a los datos del nombre y el domicilio de los vecinos del municipio que constan en el padrón municipal, dado que se trata de datos necesarios para el ejercicio de las propias competencias en que el dato relativo al domicilio es un dato relevante, tal como requiere la LRBRL y el TRLMRLC.

- ***¿Es conforme a las previsiones de la LOPD la publicación de los datos de personas presuntamente infractoras en materia de tráfico en un diario oficial?***

La publicación de datos de personas presuntamente infractoras en materia de tráfico a las cuales no se haya podido practicar la notificación personal constituye una comunicación de datos personales a efectos de la LOPD. Esta comunicación encuentra habilitación en el artículo 59.5 de la LRJPAC, mientras no entre en vigor el nuevo sistema de notificaciones electrónicas y el tablón electrónico de edictos de sanciones de tráfico.

Puede resultar adecuado a la LOPD publicar los datos relativos al nombre y apellidos de la persona infractora y, si procede, con las cuatro últimas cifras del número de DNI, junto con una identificación del número de expediente y una referencia sucinta al trámite que se notifica.

- ***¿La difusión de información que contenga datos personales en las sedes electrónicas o páginas web de los entes locales, se encuentra sometida a la normativa sobre protección de datos?***

Sí. La difusión, entendida como la comunicación de información que contiene datos personales a través de Internet, intranet o extranet, dirigida a una pluralidad indeterminada de destinatarios, se debe considerar como cesión o comunicación de datos a los efectos de la LOPD y, por lo tanto, está sometida a esta normativa.

- ***¿Puede un ayuntamiento difundir, en su página web, los datos personales contenidos en las actas de las sesiones del pleno?***

Cuando las actas incluyen datos personales, su difusión constituye un tratamiento de datos sometido a la LOPD. De acuerdo con el artículo 10.2 de la LUMESPC, se pueden difundir sin contar con el consentimiento de la persona interesada los datos referentes a actos debatidos en el pleno de la corporación o a disposiciones objeto de publicación en el boletín oficial correspondiente, teniendo en cuenta los principios y garantías que establece la normativa de protección de datos y la de protección del derecho al honor y la intimidad. En el resto de supuestos, sin perjuicio del que dispongan otras leyes, la publicación únicamente es posible si se cuenta con el consentimiento o los datos no se pueden, en ningún caso, vincular a la persona interesada.

- ***¿Se adecua a la LOPD la posibilidad de que un ciudadano consulte sus datos correspondientes en el censo electoral a través de la página web del ayuntamiento?***

Sí, si el acceso se limita a los propios datos. No constituye una cesión de datos, dado que el ciudadano que accede a la web y solicita la información sólo recibe la correspondiente a su persona. Por lo tanto, se puede consultar siempre que se

implanten las medidas de seguridad adecuadas para comprobar la identidad de quién hace la consulta.

- ***¿Puede un ayuntamiento enviar periódicamente a la Generalitat una relación de los vecinos que tengan deudas pendientes con la tesorería municipal para que les sea denegada cualquier subvención que soliciten?***

  No, porque se trata de finalidades diferentes. No obstante, se pueden comunicar, a petición del ente requirente, si la persona afectada lo ha autorizado o lo ha declarado en una declaración responsable.

Normativa aplicable: arts. 3.i), 11, 21 y 27 LOPD; 5.1.c) ,10 RLOPD; Recomendación 1/2008; 69 y ss. LRBRL; 154 y ss. TRLMRLC; 35 Ley 26/2010.

4.2.2 El encargado del tratamiento

No se considera comunicación de datos el acceso de un tercero a los datos de carácter personal, cuando este acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

Esta prestación debe estar regulada por un contrato o acuerdo de encargo, por escrito o en alguna otra forma que permita acreditar la celebración y contenido, el cual debe establecer:

a) Que únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.

b) Que no utilizará los datos con una finalidad diferente de la predeterminada en el contrato.

c) Que no comunicará los datos, ni siquiera para su conservación, a terceras personas.

d) Las medidas de seguridad.

ENCARGADO DEL TRATAMIENTO

Persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que lo vincula y delimita el ámbito de su actuación para la prestación de un servicio. También pueden ser encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

En los contratos sometidos a la legislación de contratos del sector público, el acuerdo o contrato de encargo debe constar necesariamente **por escrito**.

En caso de que el encargado del tratamiento **incumpla** alguna de estas obligaciones, se considerará como responsable del tratamiento y le serán imputables, personalmente, las infracciones que haya cometido.

Una vez cumplida la prestación contractual, los datos se tienen que **destruir o restituir** al responsable del tratamiento o al encargado que haya designado.

- ✓ En los casos en que haya una previsión legal que exija la conservación, se tienen que restituir al responsable garantizando la conservación.

- ✓ El encargado puede conservar los datos, debidamente bloqueados, para atender posibles responsabilidades.

Para el análisis de esta figura con más detalle, nos remitimos a la Recomendación 1/2010.

- ***¿Quién es el responsable del fichero que contiene los datos relativos a la recaudación de los tributos locales, cuando esta función la lleva a cabo una entidad colaboradora por cuenta de un ayuntamiento?***

  El responsable del fichero es el ayuntamiento correspondiente, mientras que el recaudador es un encargado del tratamiento, siempre que se suscriba el correspondiente contrato o acuerdo de encargo, de acuerdo con el artículo 12 de la LOPD.

- ***¿Puede un ayuntamiento comunicar los datos relativos a la titularidad de los bienes inmuebles situados en el término municipal a una empresa concesionaria del servicio de suministro de agua potable?***

  Sí, siempre que se suscriba el correspondiente contrato o acuerdo de encargo, de acuerdo con el artículo 12 de la LOPD.

- ***¿Para que un ente instrumental trate datos por cuenta de un ayuntamiento, es suficiente que éste le dé ciertas indicaciones o instrucciones?***

  No. Cuando el ente instrumental accede, por cuenta del ayuntamiento, a datos personales que se tratan bajo la responsabilidad del ayuntamiento, tiene que hacerlo a través del correspondiente contrato, convenio o acuerdo, en los términos del artículo 12 de la LOPD.

Normativa aplicable: arts. 3.g), 9 y 12 LOPD; D.A. 26 TRLCSP; 20 y ss, 82 RLOPD; Recomendación 1/2010.

4.2.3 Acceso de los concejales a información municipal

El acceso a información municipal que contiene datos personales por parte de los concejales no es propiamente un supuesto de cesión o comunicación de datos, en los términos del artículo 3.i) de la LOPD, dado que un concejal, que es parte integrante del consistorio, no puede ser considerado como un tercero ajeno a la relación que se establece entre el ayuntamiento y la persona titular de los datos personales.

La normativa aplicable otorga a los concejales municipales un derecho de acceso específico a la información del ayuntamiento, para el ejercicio de las funciones que les corresponden.

La concurrencia de este derecho específico con el derecho a la protección de datos personales requiere ponderar si el acceso a información por parte de los concejales es

necesario para desarrollar las funciones que tienen atribuidas. Eso hace especialmente relevante la aplicación del principio de calidad.

Cuando los concejales acceden a datos personales incluidos en la información municipal, quedan sujetos a los principios y obligaciones de la LOPD, entre otros el deber de secreto.

- ***¿Pueden los concejales de la oposición acceder a información municipal?***

  Sí. La normativa aplicable otorga a todos los miembros de las corporaciones locales, independientemente de que formen parte del gobierno municipal o de la oposición, el derecho a obtener del alcalde o alcaldesa, o del presidente o presidenta, o de la comisión de gobierno, los antecedentes, datos o informaciones en poder de los servicios de la corporación que resulten necesarios para desarrollar las funciones que cada concejal tenga encomendadas.

- ***¿Pueden los concejales acceder a los datos de carácter personal del padrón municipal de habitantes? ¿Pueden acceder para cualquier finalidad?***

  Los concejales, como miembros de la corporación, pueden acceder a los datos de los ficheros de ésta, entre los cuales el fichero del padrón municipal de habitantes, sin previo consentimiento de los afectados, siempre que sea necesario para el desarrollo de las funciones que les atribuye la legislación de régimen local.

  Los concejales no pueden acceder a la información para el ejercicio de finalidades no relacionadas con el ejercicio de sus funciones, como podrían ser, entre otros, las propias de la actividad política del partido al cual pertenecen.

- ***¿Los concejales tienen que justificar el motivo de su petición de acceso a información municipal?***

  Como se desprende de la LRBRL y de la jurisprudencia del Tribunal Supremo, a los concejales no se les exige que expliquen o fundamenten la finalidad de su petición de acceso a la información, que se entiende implícita en el ejercicio de sus funciones. No obstante, cuando la petición pueda entrar en conflicto con otros derechos, puesto que el ayuntamiento tiene que hacer una ponderación en que se tienen que tener en cuenta la finalidad, las circunstancias del caso, los datos personales afectados, etc., es conveniente y recomendable que los concejales concreten la finalidad de su petición.

Normativa aplicable: arts. 4 y 10 LOPD; 19.1, 77 LRBRL; 164 TRLMRLC.

4.2.4 Acceso de otras áreas del ayuntamiento a información municipal

Los órganos o las áreas del ayuntamiento forman parte de la administración municipal, que actúa bajo una personalidad jurídica única. Por lo tanto, las informaciones que circulen entre estos diferentes órganos no tienen, desde el punto de vista de la normativa de protección de datos, la consideración de comunicación. Todo esto sin perjuicio que la utilización de los datos por parte de otros órganos o áreas, diferentes a aquéllas que las recogieron, está sometida al principio de finalidad.

4.2.5 Transferencias internacionales de datos

Son transferencias internacionales de datos todas las comunicaciones de datos con un destinatario situado fuera del territorio del espacio económico europeo.

Este tipo de comunicaciones requieren que la legislación del país destinatario proporcione un nivel adecuado de protección. De lo contrario, es necesario obtener autorización del director o directora de la Agencia Española de Protección de Datos.

No obstante, la normativa establece una serie de supuestos en que se permite la transferencia internacional de datos sin necesidad de autorización:

a) Cuando resulte de la aplicación de un tratado o convenio del cual España sea miembro.

b) Cuando tenga por objeto dar o solicitar auxilio judicial internacional.

c) Cuando sea necesaria para el diagnóstico o la asistencia sanitaria.

d) Cuando haga referencia a transferencias dinerarias.

e) Cuando la persona afectada haya dado su consentimiento inequívoco.

f) Cuando sea necesario para ejecutar un contrato entre la persona afectada y el responsable del fichero, o entre éste último y un tercero cuando sea en interés de la persona afectada.

g) Cuando sea necesaria o legalmente exigida para salvaguardar un interés público.

h) Cuando se requiera para el ejercicio de un derecho dentro de un procedimiento judicial.

i) Cuando la petición la efectúe una persona con un interés legítimo desde un Registro público.

Normativa aplicable: arts. 20.2.e), 33 y 34 LOPD; 54.1.e), 65 y ss, 137 y ss. RLOPD.

4.3 Los derechos de *habeas data*

Las personas titulares de los datos, como parte de su derecho a la autodeterminación informativa, disponen de los derechos de acceso, rectificación, cancelación y oposición. Estos derechos, conocidos como derechos de *habeas data* o con el acrónimo de derechos ARCO, se caracterizan por ser:

a) **Personalísimos**: sólo los puede ejercer la persona titular de los datos, salvo los supuestos siguientes:

- Cuando la persona afectada se encuentre en situación de incapacidad o minoría de edad, que le imposibilite el ejercicio de estos derechos, los puede ejercitar el representante legal.

- Cuando se actúe mediante un representante voluntario:

  - ✓ Si se trata de ficheros privados, hay que aportar copia del DNI o equivalente y de la representación conferida. La utilización de firma electrónica identificativa de la persona afectada exime de la presentación de las fotocopias del DNI o documento equivalente.

  - ✓ Si se trata de ficheros de las administraciones publicas, se tiene que acreditar la representación por cualquier medio válido en derecho, que deje constancia fidedigna, o mediante la comparecencia personal de la persona afectada.

b) **Independientes**: en ningún caso el ejercicio de uno de estos derechos constituye un requisito previo para el ejercicio de otro.

c) **Gratuitos**: el ejercicio de estos derechos se debe poder realizar por un medio sencillo y no puede suponer un ingreso adicional para el responsable del tratamiento.

El ejercicio de los derechos ARCO puede verse modulado por motivos de seguridad pública o relativos a la hacienda pública, en los casos previstos legalmente.

Normativa aplicable: arts. 15-18 y 22-23 LOPD.

4.3.1 Derecho de acceso

Mediante este derecho, la persona afectada tiene derecho a conocer:

- Los datos de carácter personal que sean objeto de tratamiento.
- La finalidad del tratamiento.
- El origen de estos datos.
- Las comunicaciones que se han hecho o que se han previsto hacer.

El derecho se puede ejercer en relación con datos concretos, datos incluidos en un determinado fichero o la totalidad de sus datos sometidos a tratamiento.

- ✓ En casos de especial complejidad, el responsable del fichero puede facilitar a la persona afectada una lista de sus ficheros y pedirle que especifique respecto de cuáles pretende ejercer su derecho.

- ✓ El responsable del fichero dispone de 30 días a partir de la recepción de la solicitud, para notificar la respuesta a la persona afectada. Si la resolución es estimatoria, hay que hacer efectivo el acceso en el plazo de 10 días.

- ✓ El responsable del fichero puede denegar el acceso, en los casos en que ya se haya ejercido el mismo derecho en los doce meses anteriores a la solicitud, a menos que la persona interesada acredite un interés legítimo que lo justifique.

La persona afectada puede pedir que el derecho de acceso se haga efectivo a través de los **sistemas de consulta** siguientes:

- Visualización en pantalla.
- Escrito, copia o fotocopia, por correo certificado u ordinario.
- Correo electrónico u otros sistemas de comunicación electrónica.
- Cualquier otro sistema que sea adecuado a las características del fichero.

✓ Si el responsable ofrece un determinado sistema para hacer efectivo el derecho de acceso y la persona afectada lo rechaza, el responsable no tiene que responder de los riesgos que para la seguridad de la información se puedan derivar de la elección.

✓ Si la persona afectada exige que el derecho de acceso se materialice mediante un procedimiento que implica un coste desproporcionado respecto del ofrecido por el responsable, con los mismos efectos y garantizando la misma seguridad, los gastos derivados de su elección irán a cargo de la persona afectada.

¿Es posible denegar el ejercicio del derecho de acceso por la dificultad o el elevado coste que pueda suponer a la entidad local?

No, dado que la LOPD prevé que los datos de carácter personal se tienen que almacenar de forma que permitan el ejercicio del derecho de acceso, excepto que hayan sido legalmente canceladas. Ahora bien, este derecho sólo se podrá ejercer en intervalos no inferiores de 12 meses, excepto que se acredite un interés legítimo que lo justifique.

¿Pueden los herederos ejercer el derecho de acceso?

Dado que la muerte extingue la personalidad civil, los herederos no pueden ejercer el derecho de acceso del artículo 15 de la LOPD, sin perjuicio que otras normas sí que les puedan reconocer el derecho a acceder a determinada información.

Normativa aplicable: arts. 15 LOPD; 9.2 LOVFCS; 2.4 y 27 y ss. RLOPD; 9.1 Decreto 78/2010; 15 Decreto 134/1999; 13 Instrucción 1/2009.

4.3.2 Derecho de rectificación

Mediante este derecho, la persona afectada puede pedir al responsable del fichero que rectifique los datos que sean inexactos o incompletos. La solicitud tiene que indicar el dato o los datos erróneos y la corrección correspondiente y tiene que ir acompañada de la documentación que lo justifica.

✓ El responsable del fichero tiene que resolver sobre la solicitud de rectificación en el plazo de 10 días desde su recepción.

- ✓ Si los datos rectificados se han cedido previamente, el responsable del fichero tiene que notificar al destinatario las rectificaciones efectuadas en un plazo de 10 días desde la resolución, a fin de que también las rectifique, también en un plazo de 10 días.

- ✓ No se puede hacer efectivo el derecho de rectificación cuando lo impida una ley o una norma de derecho comunitario de aplicación directa.

- ✓ No se puede hacer efectivo el derecho de rectificación cuando una ley o norma de derecho comunitario de aplicación directa impidan revelar la existencia del tratamiento.

¿Se puede ejercer el derecho de rectificación respecto de los datos que consten en los ficheros de la hacienda municipal?

Sí, se puede ejercer. No obstante, se puede denegar en aquellos casos en que el ejercicio del derecho de rectificación pueda obstaculizar las actuaciones administrativas destinadas a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando la persona afectada sea objeto de actuaciones inspectoras.

Con respecto a los datos relativos al domicilio fiscal, no se pueden modificar a menos que éste no coincida con el domicilio fiscal declarado por la persona afectada, visto lo que dispone el artículo 48 de la Ley General Tributaria.

Normativa aplicable: arts. 16, 23.2 LOPD; 31 y ss. RLOPD; 14 Instrucción 1/2009.

4.3.3 Derecho de cancelación

Mediante este derecho, la persona afectada puede pedir al responsable del fichero que suprima los datos que sean inadecuados o excesivos. La solicitud tiene que indicar los datos a que se refiere y tiene que ir acompañada de la documentación que lo justifica.

- ✓ El responsable del fichero tiene que resolver sobre la solicitud de cancelación, en el plazo de 10 días desde su recepción.

- ✓ Si los datos rectificados se han cedido previamente, el responsable del fichero tiene que notificar al destinatario las rectificaciones efectuadas en un plazo de 10 días desde la resolución, a fin de que también las cancele, también en un plazo de 10 días.

- ✓ No se pueden cancelar los datos:

  - Cuando se tengan que conservar durante un periodo de tiempo por motivos legales o contractuales.
  - Cuando lo impida una ley o norma de derecho comunitario de aplicación directa.
  - Cuando una ley o norma de derecho comunitario de aplicación directa impidan al responsable revelar el tratamiento de los datos a que se refiere la cancelación.

La cancelación de los datos da lugar al bloqueo. El **bloqueo** implica que los datos se pueden conservar exclusivamente a disposición de las administraciones públicas, los juzgados y los tribunales, para atender las posibles responsabilidades nacidas del tratamiento, mientras no hayan prescrito estas responsabilidades. Una vez transcurrido este plazo se pueden suprimir los datos.

BLOQUEO

Identificación y reserva de los datos personales, con la finalidad de impedir el tratamiento excepto para ponerlos a disposición de las administraciones públicas, jueces y tribunales, para atender las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de las mencionadas responsabilidades.

- ***¿Pueden los herederos ejercer el derecho de cancelación?***

  Las personas vinculadas al difunto, por razones familiares o análogas, pueden notificar el óbito al responsable del tratamiento y solicitar la cancelación de los datos.

Normativa aplicable: arts. 16 LOPD; 9.2 LOVFCS; 2.4 y 31 y ss. RLOPD; 9.2 Decreto 78/2010; 15 Decreto 134/1999; 15 Instrucción 1/2009.

4.3.4 Derecho de oposición

El ejercicio de este derecho por parte de las personas afectadas impide a las entidades tratar sus datos personales o, si el tratamiento se hubiera iniciado anteriormente, obliga a cesar el tratamiento, en alguno de los supuestos siguientes:

- Cuando en tratamientos para los cuales no sea necesario el consentimiento de la persona afectada, haya un motivo legítimo y fundado referido a su situación personal concreta que lo justifique, siempre que una ley no disponga lo contrario.

- Cuando se trate de ficheros destinados a actividades publicitarias y de prospección comercial.

- Cuando el tratamiento tenga como finalidad la adopción de una decisión con efectos jurídicos referida a la persona afectada, basada únicamente en un tratamiento automatizado.

  ✓ El responsable del fichero tiene que resolver sobre la solicitud de oposición en el plazo de 10 días desde su recepción.

- ***¿Puede un vecino pedir que su nombre, u otros datos personales, no aparezcan en un listado que el ayuntamiento tiene que exponer públicamente por mandato legal?***

  En los casos en que no se requiere el consentimiento de la persona para tratar determinados datos, como podría ser la exposición pública de una lista de personas que los ayuntamientos tienen que exponer por mandato legal, la persona titular de los datos puede ejercer su derecho de oposición a fin de que, por motivos justificados relativos a su situación personal (como por ejemplo motivos relativos a la seguridad o la integridad física), sus datos personales no se difundan.

Normativa aplicable: arts. 6.4 LOPD; 34 y ss, 50 RLOPD; 9.3 Decreto 78/2010; 16 Instrucción 1/2009.

4.3.5 Procedimiento para ejercer los derechos ARCO

El **procedimiento** a seguir para ejercer los derechos ARCO es el siguiente:

a) Solicitud de la persona afectada dirigida al responsable del fichero o, si procede, al encargado del tratamiento (el responsable del tratamiento puede pedir la enmienda de la solicitud, en caso de que no se cumplan los requisitos establecidos en el artículo. 25.1.a) del RLOPD).

- ✓ Conviene hacerlo con un medio que permita acreditar la recepción de la solicitud.
- ✓ Cuando la entidad responsable disponga de un servicio de atención al público o de ejercicio de reclamaciones, la persona afectada se puede dirigir a dicho servicio con el fin de ejercer sus derechos ARCO.
- ✓ Los derechos se pueden ejercer también delante del encargado del tratamiento. En este caso, el encargado tiene que trasladar la solicitud al responsable del fichero para que la resuelva, excepto en los casos en que el contrato de encargado del tratamiento lo habilite para resolver las solicitudes por cuenta del responsable.

b) El responsable del fichero debe contestar la solicitud, con independencia que en el fichero figuren o no datos personales de quien ha presentado la solicitud, dentro del plazo establecido:

- Derecho de acceso: 30 días
- Resto de derechos: 10 días

El responsable del fichero tiene que formar los miembros de su organización para que puedan informar del procedimiento de ejercicio de los derechos ARCO y, si procede, tramitarlos de forma diligente.

- ***¿Se debe atender la solicitud de las personas afectadas que no hayan utilizado el medio establecido por el responsable?***

  Sí, siempre que se haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud en los términos del artículo 25.1 RLOPD.

- ***¿Es necesario responder la solicitud cuando ya se hayan destruido los datos?***

  Sí, las solicitudes de ejercicio de los derechos siempre se tienen que responder de forma expresa y dentro del plazo establecido.

Normativa aplicable: arts. 17 LOPD; 25, 44, 50, 117 y ss. RLOPD; 17 Instrucción 1/2009.

4.3.6 Reclamación de tutela de derechos

La tutela de derechos se ejerce mediante un procedimiento que se tramita ante la Autoridad Catalana de Protección de Datos y que se inicia a instancia de la persona afectada:

- Para ejercer sus derechos el ciudadano se tiene que dirigir al responsable del fichero. En caso de que no se dé respuesta a esta petición dentro del plazo legalmente establecido, o se deniegue el ejercicio de uno de estos derechos, se puede dirigir a la Autoridad Catalana de Protección de Datos mediante una reclamación de tutela de derechos.

- La Autoridad traslada la reclamación al responsable del fichero y, una vez recibidas las alegaciones dentro del plazo legalmente establecido y practicadas todas las pruebas, tiene que dictar y notificar una resolución que resuelva sobre la reclamación, en el plazo de seis meses desde la fecha de entrada de la reclamación. Si no se resuelve dentro de este plazo, la reclamación de tutela se considera desestimada por silencio administrativo.

- Cuando la resolución de la reclamación sea estimatoria, hay que requerir al responsable del fichero para que, en el plazo de los 10 días siguientes a la notificación, haga efectivo el ejercicio del derecho reclamado.

Normativa aplicable: arts. 18 LOPD; 5. b) y 16 LACPD; 117 y ss. RLOPD.

4.4 Medidas de seguridad

4.4.1 Implementación de las medidas de seguridad

Un tratamiento correcto de los datos personales requiere que responsables y encargados del tratamiento implementen una serie de medidas de seguridad, adecuadas a las diferentes tipologías de datos que se tratan.

Corresponde al **responsable** del fichero y, si procede, al responsable del tratamiento, adoptar las medidas necesarias en cada caso, teniendo en cuenta el estado de la tecnología, la naturaleza de los datos almacenados, el sistema de tratamiento utilizado (automatizado o no) y los riesgos a los que estén expuestos, ya sean provenientes de la acción humana o del medio físico o natural. Cuando exista un **encargado del tratamiento**, le son de aplicación las mismas obligaciones relativas a las medidas de seguridad que al responsable, de acuerdo con lo que se establezca en el contrato de encargo del tratamiento.

Las medidas de seguridad pueden ser tanto de carácter técnico como organizativo y están destinadas a evitar la alteración, la pérdida o el acceso a los datos de carácter personal por parte de terceros no autorizados.

El RLOPD establece las medidas necesarias de acuerdo con el tipo de datos tratados y el soporte en el cual estén almacenados. Las medidas de seguridad se **clasifican en tres niveles de seguridad** que tienen la condición de mínimos exigibles:

- **Básico**: las tienen que adoptar todos los ficheros o tratamientos de datos personales.

- **Medio**: se aplican, junto con las de nivel básico, a los ficheros o tratamientos que tengan por objeto datos relativos a:

  a) La comisión de infracciones administrativas o penales.

  b) Información sobre la solvencia patrimonial i crédito que traten entidades que presten estos servicios.

  c) El ejercicio de potestades tributarias por parte de administraciones tributarias.

  d) La prestación de servicios financieros por entidades financieras.

  e) El ejercicio de competencias de las entidades gestoras de la seguridad social y mutuas de accidentes de trabajo y enfermedades profesionales.

  f) La evaluación de la personalidad o el comportamiento de los individuos.

  Los ficheros de los operadores de servicios de comunicaciones electrónicas disponibles al público o redes públicas de comunicaciones electrónicas, que contengan datos relativos al tráfico y la localización, tienen que adoptar medidas de nivel medio además de la implantación de un registro de accesos.

- **Alto**: Se aplican, junto con las de nivel básico y medio, a los ficheros o tratamientos que contengan datos relativos a:

  a) Ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

  b) Recogidos para finalidades policiales, sin el consentimiento de las personas afectadas.

  c) Actos de violencia de género.

La determinación del nivel de seguridad aplicable dependerá de los datos que se recojan en cada caso. **A título orientativo,** algunos de los ficheros más característicos de los entes locales podrían tener asignado el nivel de seguridad siguiente:

FICHEROS	NIVEL DE SEGURIDAD
Padrón municipal	Básico
Registro municipal de intereses	Medio
Recursos humanos	Medio
Infracciones administrativas	Medio
Hacienda Pública	Medio
Policial	Alto
Registro entrada y salida de documentos	Alto

- ***¿Qué nivel de seguridad requieren los datos relativos a la afiliación sindical, cuando se recojan exclusivamente para hacer una transferencia de las cuotas sindicales al sindicato correspondiente?***

  Básico o medio, de acuerdo con el resto de datos que contenga el fichero. De acuerdo con el art. 81.5.a) RLOPD no es exigible aplicar medidas de nivel alto a los datos que, a pesar de tener asignado en principio este nivel, se utilicen con la única finalidad de hacer una transferencia dineraria a las entidades en que los afectados sean asociados o miembros.

- ***¿Qué nivel de seguridad requieren los datos relativos a la condición de discapacidad o invalidez de la persona afectada o al grado de la discapacidad?***

  Básico o medio, de acuerdo con el resto de datos que contenga el fichero, siempre que el dato se trate para el cumplimiento de un deber público. De acuerdo con el art. 81.6) RLOPD, no es exigible aplicar medidas de nivel alto en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez de la persona afectada, con motivo del cumplimiento de deberes públicos.

- ***¿Cómo se aplican las medidas de seguridad en los ficheros de videovigilancia?***

  De conformidad con el art. 20.2 de la Instrucción 1/2009, los ficheros de videovigilancia requieren, con carácter general, el nivel de seguridad básico, sin perjuicio que en determinados supuestos puedan ser de aplicación medidas de seguridad de nivel medio o alto.

  En las imágenes, y si procede, a la voz, obtenidas o tratadas mediante sistemas digitales, se les tiene que aplicar las medidas de seguridad previstas en la LOPD para los tratamientos automatizados, mientras que en los que no utilicen tecnología digital, o que posteriormente a la captación se incorporen a soportes que no se basen en la tecnología digital, se les tiene que aplicar las medidas de seguridad previstas para los ficheros no automatizados.

- ***¿En relación a los ficheros de videovigilancia, en qué casos se han de hacer copias de seguridad?***

  Si los datos se guardan por un periodo superior a una semana, se debe hacer copias de seguridad semanalmente, según dispone el artículo 21.4.e) de la Instrucción 1/2009.

Normativa aplicable: arts. 9,12 y 20.2.h) LOPD; 54.1.h), 79 y ss, 89 y ss, 105 y ss. RLOPD; 19, 20 y 21 Instrucción 1/2009.

FICHEROS Y TRATAMIENTOS AUTOMATIZADOS			
MEDIDAS	**NIVEL BÁSICO**	**NIVEL MEDIO**	**NIVEL ALTO**
Funciones y obligaciones del personal	Art. 89	Art. 89	Art. 89
Registro de incidencias	Art. 90	Art. 100	Art. 100
Control de acceso	Art. 91	Art. 99	Art. 99
Gestión de soportes y documentos	Art. 92	Art. 97	Art. 101
Identificación y autentificación	Art. 93	Art. 98	Art. 98
Copias de seguridad y recuperación	Art. 94	Art. 94	Art. 102
Responsable de seguridad		Art. 95	Art. 95
Auditoría		Art. 96	Art. 96
Control de acceso físico		Art. 99	Art. 99
Registro de accesos			Art. 103
Telecomunicaciones			Art.104

Normativa aplicable: art. 89 y ss. RLOPD.

FICHEROS Y TRATAMIENTOS NO AUTOMATIZADOS			
MEDIDAS	**NIVEL BÁSICO**	**NIVEL MEDIO**	**NIVEL ALTO**
Criterios de archivo	Art. 106	Art. 106	Art. 106
Dispositivos de almacenamiento	Art. 107	Art. 107	Art. 107
Custodia de los soportes	Art. 108	Art. 108	Art. 108
Responsable de seguridad		Art. 109	Art. 109
Auditoría		Art. 110	Art. 110
Almacenaje de la información			Art. 111
Copia o reproducción			Art. 112
Acceso a la documentación			Art. 113
Traslado de documentación			Art. 114

Normativa aplicable: art. 106 y ss. RLOPD.

4.4.2 Documento de seguridad

El responsable del fichero o tratamiento tiene que elaborar un **documento de seguridad,** que tiene que recoger las medidas de índole técnica y organizativa que el responsable del fichero y/o el encargado del tratamiento, si procede, tienen que implementar sobre los ficheros que contienen datos personales.

El documento de seguridad se tiene que mantener **actualizado** en todo momento y tiene que ser objeto de revisión siempre que se produzcan cambios relevantes que puedan repercutir en el cumplimiento de las medidas de seguridad implementadas.

El documento de seguridad tiene que tener el contenido mínimo que detalla el artículo 88.3 del RLOPD:

a) Ámbito de aplicación del documento, con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el RLOPD.

c) Funciones y obligaciones del personal, en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Procedimientos de realización de copias de seguridad y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Medidas a adoptar para el transporte de soportes y documentos, así como para destruir los documentos y los soportes o, si procede, reutilizarlos.

- ***¿Tratándose de un fichero público, hay que tener en cuenta también la normativa de archivos?***

  Sí. En el documento de seguridad hay que indicar el criterio de archivo utilizado, con sujeción a los criterios contenidos en la normativa de archivos.

Normativa aplicable: arts. 88 RLOPD; 22 Instrucción 1/2009.

5

EL RÉGIMEN DE RESPONSABILIDAD

El incumplimiento de la normativa de protección de datos puede dar lugar a una serie de responsabilidades, a las cuales el responsable y el encargado del tratamiento tienen que hacer frente

Sin perjuicio de las responsabilidades que se puedan derivar de la vulneración de otros derechos, como el derecho al honor, a la intimidad y a la propia imagen, la vulneración del derecho a la protección de datos genera responsabilidades que se pueden exigir mediante denuncia delante la Autoridad Catalana de Protección de Datos, cuando los hechos sean constitutivos de alguna de las infracciones tipificadas en la LOPD o mediante una reclamación de responsabilidad por los daños y perjuicios sufridos.

5.1 Tipos de responsabilidades

Las responsabilidades derivadas de un tratamiento ilícito de los datos personales pueden ser de diferentes tipos:

Responsabilidad patrimonial: Si las personas titulares de los datos personales sufren algún daño o alguna lesión en sus derechos o intereses, a consecuencia de la vulneración de lo que dispone la normativa de protección de datos, tienen derecho a ser indemnizados. La responsabilidad patrimonial por vulneración de la LOPD puede reclamarse en vía administrativa, de acuerdo con la legislación reguladora del régimen de responsabilidad patrimonial de las administraciones públicas, cuando el perjuicio provenga de ficheros o tratamientos de titularidad pública, o bien ante los tribunales ordinarios, en relación con ficheros o tratamientos de titularidad privada.

Responsabilidad penal: El Código Penal tipifica como delito contra la intimidad el descubrimiento y la revelación de secretos. Se tipifican, entre otros, el apoderamiento, la utilización o la modificación, así como la difusión o cesión, sin consentimiento y en perjuicio de terceras personas, de datos reservados de carácter personal o familiar, que se encuentren en ficheros o soportes informáticos, electrónicos o telemáticos, o en archivos o registros, tanto públicos como privados.

Responsabilidad administrativa: Los responsables de los ficheros y los encargados del tratamiento, tanto de titularidad pública como privada, están sujetos al régimen sancionador de la LOPD. La Autoridad Catalana de Protección de Datos aplica este régimen sancionador, en relación con ficheros de titularidad pública y privada, dentro de su ámbito competencial.

- ***¿Las personas interesadas pueden reclamar una indemnización por los daños o las lesiones sufridas como consecuencia del incumplimiento de la normativa de protección de datos?***

  Sí. Tratándose de un fichero de titularidad pública, pueden ejercer una acción de reclamación de responsabilidad, de acuerdo con la legislación reguladora del régimen de responsabilidad patrimonial de las administraciones públicas, ante el ente local responsable y, si procede, ante la jurisdicción contenciosa administrativa.

Normativa aplicable: arts. 19 LOPD; 139 y ss. LRJPAC; 1902 CC; 197 y ss. C.P.

5.2 Potestad de inspección

En el marco de un procedimiento sancionador o antes de iniciarlo, la Autoridad puede inspeccionar, si lo considera necesario, los ficheros y tratamientos de datos personales, con el fin de obtener todas las informaciones necesarias para verificar el cumplimiento de la normativa en materia de protección de datos. En concreto, la Autoridad puede solicitar la presentación o el envío de documentos y de datos o examinarlos en el lugar donde estén depositados. También puede inspeccionar los equipos físicos y lógicos utilizados, para lo cual puede acceder a los locales donde estén instalados.

Los funcionarios que ejercen la función inspectora tienen la consideración de autoridad pública, están vinculados por el deber de secreto en sus actuaciones y tienen que contar con el auxilio, preferente y urgente, de las entidades inspeccionadas.

Los hechos constatados por los funcionarios de la Autoridad, y formalizados en documento público, tienen valor probatorio, sin perjuicio de las otras pruebas que puedan aportar las personas interesadas.

Normativa aplicable: arts. 40 LOPD; art. 5.j) y 19 LACPD.

5.3 Potestad de inmovilización de ficheros

En supuestos de infracción grave o muy grave, en caso de utilización o de comunicación ilícita de datos personales en que se atente gravemente contra los derechos fundamentales y las libertades públicas de los ciudadanos o se impida su ejercicio, la Autoridad puede exigir a los responsables de los ficheros el cese de la utilización o la comunicación ilícita de datos personales. Si no se atiende el requerimiento, se pueden inmovilizar los ficheros con el fin de restaurar los derechos de las personas afectadas. La inmovilización queda sin efecto si en el plazo de 15 días no se acuerda la incoación de un procedimiento sancionador y no se ratifica la medida.

Normativa aplicable: arts. 49 LOPD; 25 LACPD.

5.4 Infracciones

El artículo 44 de la LOPD tipifica las infracciones en que pueden incurrir los responsables de los ficheros y los encargados del tratamiento, que pueden ser **leves, graves y muy graves**:

LEVES	GRAVES	MUY GRAVES
No enviar a la APDCAT las notificaciones previstas en la LOPD o en el RLOPD (44.2.a)	Crear ficheros de titularidad pública o iniciar la recogida de datos sin autorización de disposición general publicada en el DOGC o BOP correspondiente (44.3.a)	Recoger datos de manera engañosa o fraudulenta (44.4.a)
No solicitar la inscripción del fichero en el Registro de Protección de Datos de Cataluña	Tratar datos sin tener el consentimiento de la persona afectada, cuando sea necesario	Tratar o ceder los datos especialmente protegidos de los apartados 2, 3 y 5 del

(44.2.b)	según la LOPD y el RLOPD (44.3.b)	artículo 7 LOPD, excepto en los supuestos que la LOPD lo autorice, o violentar la prohibición del artículo 7.4 LOPD (44.4 b)
Incumplir con el deber de información a la persona afectada sobre el tratamiento de sus datos personales, cuando los datos se recojan de la misma persona interesada (44.2.c)	Tratar datos o utilizarlos posteriormente con conculcación de los principios y garantías establecidas en el art. 4 LOPD y en el RLOPD, excepto que sea constitutivo de infracción muy grave (44.3.c)	No cesar en el tratamiento ilícito de datos cuando haya un requerimiento previo del director/a de la APDCAT (44.4.c)
Transmitir datos a un encargado del tratamiento sin cumplir con los deberes formales del art. 12 LOPD (44.2.d)	Vulnerar el deber de guardar secreto sobre el tratamiento de los datos a que se refiere el art. 10 LOPD (44.3 d)	Transferir datos a países que no proporcionen un nivel de protección equiparable sin autorización del director/a de la AEPD, excepto que no sea necesaria según la LOPD o RLOPD (44.4.d)
	Impedir u obstaculizar el ejercicio de los derechos ARCO (44.3.e)	
	Incumplir el deber de información a la persona afectada sobre el tratamiento de sus datos, cuando no se hayan conseguido de la misma persona interesada (44.3.f)	
	Incumplir el resto de deberes de notificación o requerimiento de la persona afectada impuestos por la LOPD y el RLOPD (44.3.g)	
	Mantener los ficheros, locales, programas o equipos que contengan datos sin las debidas condiciones de seguridad que determina el RLOPD (44.3.h)	
	No atender requerimientos o advertencias de la APDCAT o no proporcionarle todos los documentos o información que solicite (44.3.i)	
	Obstruir el ejercicio de la función inspectora (44.3.j)	
	Comunicar o ceder los datos sin contar con legitimación para ello, de acuerdo con la LOPD y el RLOPD, a menos que sea constitutiva de infracción muy grave (44.3.k)	

La prescripción:

Las infracciones previstas en la LOPD prescriben en los plazos siguientes:

a) Infracciones **muy graves**: tres años.

b) Infracciones **graves:** dos años.

c) Infracciones **leves:** un año.

El plazo de prescripción de las infracciones empieza a contar el día en que se haya cometido la infracción. Se interrumpe por la iniciación del procedimiento sancionador con conocimiento de la persona interesada, y se reanuda si el expediente está paralizado durante más de seis meses por causa no imputable al presunto infractor.

Normativa aplicable: art. 44, 46 y 47 LOPD.

5.5 Sanciones

Con respecto a las infracciones cometidas en relación con los ficheros de **titularidad privada** o con información que tendría que estar incluida en ficheros de esta naturaleza, la comisión de una infracción tipificada en la LOPD comporta, junto con el requerimiento de adopción de las medidas correctoras apropiadas, la imposición de la sanción correspondiente:

a) Infracciones **leves:** multa de 900 a 40.000 €

b) Infracciones **graves:** multa de 40.001 a 300.000 €

c) Infracciones **muy graves:** multa de 300.001 a 600.000 €

De forma excepcional, en supuestos en que no haya reincidencia y siempre que concurran determinadas circunstancias, la Autoridad puede formular una advertencia e imponer al responsable la adopción de determinadas medidas correctoras, en lugar de abrir un procedimiento sancionador.

Con respecto a las infracciones cometidas en relación con ficheros de **titularidad pública**, no comportan la imposición de ningún tipo de sanción. En este caso, la Autoridad dicta una resolución en que declara la infracción y establece las medidas que hay que adoptar para que cesen o se corrijan los efectos de la infracción. En este caso, la Autoridad también puede proponer la iniciación de actuaciones disciplinarias, si son procedentes.

Las sanciones previstas en la LOPD prescriben en los plazos siguientes:

a) Sanciones por infracciones **muy graves**: tres años.

b) Sanciones por infracciones **graves:** dos años.

c) Sanciones por infracciones **leves:** un año.

El cómputo del plazo de prescripción de las sanciones empieza al día siguiente del día en que adquiere firmeza la resolución por la cual se impone la sanción. Se interrumpe por la iniciación del procedimiento de ejecución con conocimiento de la persona interesada, y se reanuda si el procedimiento de ejecución está paralizado durante más de seis meses por una causa no imputable al infractor.

Normativa aplicable: arts. 37. g), 45-47 LOPD; 5.k), 18, 21-24 LACPD.

5.6 Procedimiento sancionador

La Autoridad Catalana de Protección de Datos, en la tramitación de los procedimientos sancionadores y también en los procedimientos de declaración de infracciones cometidas en relación con ficheros de titularidad pública, tiene que seguir el procedimiento sancionador aplicable a los ámbitos de competencia de la Generalitat.

Actuaciones previas: Con carácter previo a la iniciación del procedimiento, se pueden llevar a cabo actuaciones previas para determinar si se dan circunstancias que lo justifiquen.

Si de las actuaciones previas no se derivan hechos susceptibles de motivar la imputación de ninguna infracción, se dicta resolución de archivo. Si hay indicios susceptibles de motivar la imputación de una infracción, se dicta acuerdo de inicio del procedimiento sancionador o de declaración de infracción.

Iniciación: El procedimiento sancionador se inicia de oficio, por denuncia o como consecuencia de informaciones conocidas directamente por la Autoridad.

Notificación y publicación de la resolución: en el caso de infracciones cometidas con relación a ficheros de titularidad pública, la resolución se tiene que notificar a la persona responsable del fichero o del tratamiento, al encargado del tratamiento, si procede, al órgano del cual dependan y a las personas afectadas, si las hay.

En el caso de infracciones cometidas con relación a ficheros de titularidad privada, se notifica a la persona responsable del fichero o del tratamiento, al encargado del tratamiento, si procede, y a las personas afectadas, si las hay.

La persona denunciante tiene derecho a que le comuniquen las actuaciones que se derivan de la denuncia, sin perjuicio de los derechos que pueda tener como persona interesada.

Una vez notificada a las personas interesadas, la resolución sancionadora se comunica al Síndic de Greuges y se hace pública en la web de la Autoridad, previa anonimización de los datos de carácter personal, a menos que no tenga ningún interés doctrinal o que, a pesar de la anonimización, sea aconsejable por causas justificadas evitar la publicidad para impedir que determinadas personas resulten reconocibles.

Régimen de recursos: las resoluciones sancionadoras y de declaración de infracción de la Autoridad agotan la vía administrativa y son susceptibles de recurso de reposición o directamente recurso contencioso administrativo.

Normativa aplicable: arts. 37. g), 43, 46 y 48 LOPD; 3.c), 5.k), 17, 18, 19, 21 y ss. LACPD; Decreto 278/1993.

6

LOS CÓDIGOS TIPO

La adopción de medidas proactivas, como la probación de códigos tipo, facilita el cumplimiento de la normativa de protección de datos y mejora la confianza de los ciudadanos en el tratamiento que tendrán sus datos por parte de las administraciones públicas

El cumplimiento de los principios, las obligaciones y las garantías establecidas en materia de protección de datos requiere adaptar las previsiones establecidas de forma general a la normativa, a las características y a las necesidades de cada tipo de entidad. Eso se puede hacer mediante los códigos tipo. Este mecanismo de autorregulación, promovido por los mismos entes locales o por entidades que los agrupen, establecerá la forma como se deberían cumplir los principios, las obligaciones y las garantías establecidas en la normativa, como también los compromisos adicionales que se consideren necesarios para una mejor garantía de los derechos de los ciudadanos.

Los códigos tipo son **acuerdos sectoriales**, **convenios administrativos** o **decisiones de empresa**, mediante los cuales los responsables de los tratamientos pueden establecer, entre otros aspectos, las condiciones de organización, el régimen de funcionamiento, los procedimientos aplicables, las normas de seguridad, las obligaciones de las personas afectadas y las garantías para ejercer sus derechos en materia de protección de datos.

Su objetivo es **adecuar** las previsiones establecidas tanto en la LOPD como en el RLOPD, a los tratamientos que efectúen las entidades durante el ejercicio de su actividad, para armonizar los tratamientos a través de reglas, protocolos o estándares, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de la normativa.

Tienen carácter de códigos deontológicos o de buena práctica profesional y son vinculantes para quien se adhiera de forma voluntaria.

- ✓ Los **entes locales** pueden adoptar códigos tipos, de acuerdo con lo establecido en las normas que les sean aplicables.

Tienen que incluir **procedimientos de supervisión,** con el fin de garantizar el cumplimiento de las obligaciones asumidas por los adheridos, y establecer un **régimen sancionador** que sea adecuado, eficaz y disuasorio.

Para que tengan la consideración de códigos tipo, estos acuerdos o convenios se deben **depositar e inscribir** en el Registro de Protección de Datos de Cataluña.

Una vez inscritos, las entidades están obligadas a:

- Mantener accesible al público información actualizada sobre las entidades promotoras, los adheridos, los procedimientos de adhesión, el contenido y los procedimientos de garantía de su cumplimiento.
- Hacer una memoria anual relativa, entre otros aspectos, a la difusión del código, la promoción de su adhesión y las actuaciones de verificación de su cumplimiento.
- Evaluar periódicamente su eficacia.

Normativa aplicable: arts. 32 LOPD; 71 y ss, 145 y ss. RLOPD; 11.2.b). LACPD

7

LA AUTORIDAD CATALANA DE PROTECCIÓN DE DATOS

La Autoridad Catalana de Protección de Datos es la autoridad de control competente respecto de los ficheros y tratamientos de datos de carácter personal llevados a cabo por los entes locales de Cataluña y los entes que dependen de ellos

7.1 Naturaleza y objeto

La Autoridad Catalana de Protección de Datos, entidad sucesora de la Agencia Catalana de Protección de Datos, es un organismo independiente que tiene por objeto garantizar, en el ámbito de las competencias de la Generalitat, los derechos a la protección de datos personales y de acceso a la información que está vinculada a ellos.

Se regula por la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos y el Decreto 48/2003, de 20 de febrero, por el cual se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, vigente en todo aquello que no se oponga a la ley mencionada.

Se configura como una institución de derecho público, con personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines, con plena autonomía orgánica y funcional, que actúa con objetividad y plena independencia de las administraciones públicas en el ejercicio de sus funciones.

Normativa aplicable: arts. 1 y 2 LACPD.

7.2 Ámbito de actuación

El ámbito de actuación de la Autoridad comprende los ficheros y los tratamientos que llevan a cabo:

- Las instituciones públicas de Cataluña.
- La Administración de la Generalitat.
- Los entes locales.
- Las entidades autónomas, los consorcios y las otras entidades de derecho público vinculadas a la Administración de la Generalitat o a los entes locales, o que dependen de ellos.
- Las entidades de derecho privado que cumplan, como mínimo, uno de los tres requisitos siguientes con relación a la Generalitat o a los entes locales, o que dependen de ellos:
  - ✓ Que su capital pertenezca mayoritariamente a dichos entes públicos.
  - ✓ Que sus ingresos presupuestarios provengan mayoritariamente de dichos entes públicos.
  - ✓ Que en sus órganos directivos los miembros designados por dichos entes públicos sean mayoría.
- Las otras entidades de derecho privado que prestan servicios públicos por medio de cualquier forma de gestión directa o indirecta, si se trata de ficheros y tratamientos vinculados a la prestación de estos servicios.

- Las universidades públicas y privadas que integran el sistema universitario catalán, y los entes que dependen de ellas.

- Las personas físicas o jurídicas que cumplen funciones públicas con relación a materias que son competencia de la Generalitat o de los entes locales, si se trata de ficheros o tratamientos destinados al ejercicio de dichas funciones y el tratamiento se lleva a cabo en Cataluña.

- Las corporaciones de derecho público que cumplen sus funciones exclusivamente en el ámbito territorial de Cataluña a los efectos de lo establecido en la LACPD.

Normativa aplicable: arts. 156 EAC; 3 LACPD.

7.3 Organización

La Autoridad dispone de dos órganos:

- El/la director/a, **que dirige la institución y ejerce su representación**.

- El **Consejo Asesor de Protección de Datos,** órgano de asesoramiento y participación de la Autoridad, constituido por representantes de las diferentes instituciones incluidas dentro de su ámbito de actuación, entre los cuales hay dos representantes de los entes locales de Cataluña, designados por el Consejo de Gobiernos Locales.

Normativa aplicable: arts. 6 y ss. LACPD; 13 y ss. Decreto 48/2003.

7.4 Funciones

La Autoridad lleva a cabo, entre otras, las funciones siguientes:

- **Atención al público y consultoría** en relación con las solicitudes de información, quejas o consultas sobre los servicios de la Autoridad y sobre la aplicación de la legislación de protección de datos de carácter personal, que pueda formular cualquier ciudadano o el personal de las entidades sometidas al ámbito de actuación de la Autoridad.

  Se puede contactar con este servicio a través de:

  - ✓ Teléfono: 902 011 710 (de 9 a 14 h, de lunes a viernes laborables).
  - ✓ Por correo electrónico: consultes.apdcat@gencat.cat
  - ✓ Por correo postal: calle de la Llacuna, 166, 7ª planta, 08018 Barcelona.
  - ✓ Por fax: 93 552 78 30.
  - ✓ Presencialmente: de 9 a 14 h, de lunes a viernes laborables.

- **Difusión** del derecho a la protección de datos de carácter personal a través de publicaciones, conferencias, cursos, seminarios y otras iniciativas. A estos efectos, la Autoridad dispone de una lista de distribución sobre sus iniciativas, la inscripción a la cual se puede solicitar enviando un correo electrónico dirigido a consultes.apdcat@gencat.cat

- **Registro**: a través del Registro de Protección de Datos de Cataluña, en el cual son objeto de inscripción:

  a) Los ficheros de datos personales, de titularidad pública o privada, incluidos dentro del ámbito de actuación de la Autoridad.

  b) Los códigos tipo formulados por las entidades incluidas dentro del ámbito de actuación de la Autoridad.

- **Elaboración de informes,** sobre los proyectos de disposiciones de carácter general de creación, modificación o supresión de ficheros y sobre disposiciones que tengan impacto en materia de protección de datos de carácter personal. En el caso de los entes locales estos informes son potestativos.

- **Elaboración de dictámenes** en relación con las consultas que formulen los representantes de las entidades de su ámbito de actuación.

- **Elaboración de recomendaciones e instrucciones,** con el fin de adecuar los ficheros y los tratamientos de datos a los principios y a las garantías que establece la legislación vigente de protección de datos.

- **Tutela** de los derechos ARCO, mediante un procedimiento de reclamación dirigido a hacer efectivos y restablecer de forma inmediata estos derechos de los ciudadanos.

- **Funciones de control**, integradas por:

  a) Los planes de auditoría, como sistema de control preventivo para verificar el cumplimiento de la normativa y recomendar o requerir a los responsables de los ficheros y tratamientos que adopten las medidas correctoras adecuadas.

  b) La potestad de inspección, por la cual la Autoridad puede inspeccionar los ficheros y los tratamientos de datos personales, con el fin de obtener las informaciones necesarias para desarrollar su actividad.

  c) La aplicación del régimen sancionador previsto en la LOPD respecto de los responsables de los ficheros y de los tratamientos incluidos dentro del ámbito de actuación de la Autoridad, y de los encargados de los tratamientos correspondientes.

  d) Los requerimientos de adecuación a la legalidad, en caso de infracciones graves o muy graves, para exigir el cese de la utilización o la comunicación ilícita de datos personales y, si procede, la potestad de inmovilización de ficheros, en caso de incumplimiento de los requerimientos de adecuación.

- **Otorgar autorizaciones**, para la exención del deber de información en la recogida de los datos o para el mantenimiento íntegro de determinados

datos, y otros que establezca la normativa, excepto las relativas a transferencias internacionales de datos, competencia del director de la Agencia Española de Protección de Datos.

Normativa aplicable: arts. 5 y 15 y ss. LACPD.

Abreviaturas

EAC: Estatuto de Autonomía de Cataluña.

CC: Código Civil

CP: Código Penal, aprobado por la Ley Orgánica 10/1995, de 23 de noviembre.

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

LOVFCS: Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

LRBRL: Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local.

LRJPAC: Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Ley 22/1998: Ley 22/1998, de 30 de diciembre, de la Carta municipal de Barcelona.

Ley 21/2000: Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y a la documentación clínica.

LA: Ley 10/2001, de 13 de julio, de archivos y documentos.

TRLCSP: Texto refundido de la Ley de Contratos del Sector Público, aprobado por el Real decreto legislativo 3/2011, de 14 de noviembre.

Ley 13/2008: Ley 13/2008, de 5 de noviembre, de la presidencia de la Generalitat y del Gobierno.

Ley 26/2010: Ley 26/2010, de 3 de agosto, de régimen jurídico y de procedimiento de las administraciones públicas de Cataluña.

LUMESPC: Ley 29/2010, de 3 de agosto, del uso de los medios electrónicos en el sector público de Cataluña.

LACPD: Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos.

TRLMRLC: Decreto legislativo 2/2003, de 28 de abril, por el que se aprueba el Texto refundido de la Ley municipal y de régimen local de Cataluña.

RLOPD: Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

ROAS: Reglamento de obras, actividades y servicios de las entidades locales, aprobado por el Decreto 179/1995, de 13 de junio.

Decreto 278/1993: Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación en los ámbitos de competencia de la Generalitat.

Decreto 134/1999: Decreto 134/1999, de 18 de mayo, de regulación de la videovigilancia por parte de la policía de la Generalitat y de las policías locales de Cataluña.

Decreto 48/2003: Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos.

Decreto 78/2010: Decreto 78/2010, de 22 de junio, sobre la instalación de dispositivos de videovigilancia en las dependencias policiales de la Generalitat.

Orden de 29 de junio de 2001: Orden de 29 de junio de 2001, de regulación de los medios por los que se informa de la existencia de videocámaras fijas instaladas por la policía de la Generalitat y las policías locales de Cataluña en lugares públicos.

Instrucción 1/2009: Instrucción 1/2009, de 10 de febrero, de la Agencia Catalana de Protección de Datos, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia.

Recomendación 1/2008: Recomendación 1/2008 de la Agencia Catalana de Protección de Datos sobre la difusión de información que contenga datos de carácter personal a través de Internet.

Recomendación 1/2010: Recomendación 1/2010 de la Agencia Catalana de Protección de Datos sobre el encargado del tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña.

Recomendación 1/2011: Recomendación 1/2011 de la Autoridad Catalana de Protección de Datos sobre la creación, modificación y supresión de ficheros de datos de carácter personal de titularidad pública.

Res. 04.04.2011 APDCAT: Resolución de 4 de abril de 2011, por la que se aprueba la modificación de los soportes normalizados para formalizar las inscripciones de los ficheros en el Registro de Protección de Datos de Cataluña (DOGC nº 5859, de 14.04.2011).