N/REF: 010436/2016

La consulta plantea la conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, del proyecto de investigación denominado CLIPS (Cloudification of Public Services in Smart Cities) incluido en el ámbito del séptimo programa marco de la Unión Europea. Según se expone en la documentación aportada el objetivo del proyecto es proporcionar a la comunidad una metodología y un conjunto de herramientas que permitan a las Administraciones Públicas y otros actores externos (empresas y ciudadanos) cooperar en la concepción y desarrollo de nuevos servicios basados en la nube, empezando por un conjunto de micro servicios básicos ya disponibles en la misma. De este modo, de una parte, las Administraciones Públicas pueden sacar partido de sus experiencias a nivel local con un despliegue más amplio de las soluciones exitosas basado en su distribución a través de la nube a otras administraciones y, de otra parte, la sociedad civil puede apoyar a la Administración pública a afrontar los desafíos que surjan y los cambios en las necesidades que conlleva el proceso de prestación de servicios públicos.

Se enumeran así los siguientes objetivos:

- Identificar un conjunto de servicios públicos locales viables sencillos relacionados con las llamadas “circunstancias de la vida” (por ejemplo, matricular un niño en un colegio, solicitar una licencia de conducir válida localmente, etc.

- Permitir a cada Administración pública piloto poner en la nube uno o más de esos servicios llamados servicios sencillos.

- Apoyar a las demás Administraciones públicas piloto para reutilizar esos servicios en nube después de una adecuada adaptación.

- Proporcionar a los ciudadanos servicios compuestos derivados de la combinación de servicios de las Administraciones públicas disponibles en la nube (servicios complejos). El interfaz o entorno de los servicios complejos estará preparado para instalarse en cada Portal de la Administración Pública que sea compatible.

- Habilitar la difusión de los denominados “micro proxies”, servicios específicos dedicados a hacer utilizables datos personales en poder de las Administraciones Públicas**.**

-permitir el uso real y la navegación de los datos abiertos disponibles por medio de "servicios innovadores”.

-implementar el escenario transfronterizo combinando toda clase de servicios publicados en la cloud.

Además, la plataforma dará a los interesados externos (por ejemplo, pequeña y mediana empresa, proveedores de servicios) la posibilidad de aprovechar el ecosistema de servicios en la nube así creado y añadir otros microservicios de valor añadido y servicios innovadores (por ejemplo, a fin de que puedan utilizarse los datos abiertos disponibles, sobre la base de los ya existentes).

En el proyecto participan diversas entidades públicas y privadas, españolas y de países europeos algunos de ellos pertenecientes al espacio económico europeo.

El Ayuntamiento de Santander va a llevar a cabo un proyecto piloto, para desarrollar bajo la arquitectura CLIPS, por una parte, un servicio que ya está a disposición de los ciudadanos online de manera tradicional, como es la solicitud de volante de empadronamiento, y, por otra, el desarrollo de varios servicios innovadores basados en consultas al padrón municipal enriquecido con información publicada proveniente del portal de datos abiertos de dicho Ayuntamiento. No obstante, con posterioridad se ha declarado que se deja sin efecto lo relativo a esta segunda parte por considerar que no resulta factible la comercialización del servicio.

El consorcio en Santander lo forma el Ayuntamiento de Santander y TST una pyme de la ciudad, ésta será quien desarrolle los microservicios y los servicios complejos que se ubicarán en la nube en el data center de Port Saint-Martin, Italia. Los datos personales serán accedidos por TST a través del microproxy que proporcionará el Ayuntamiento que en concreto estará formado por una API que permite acceder a las bases de datos municipales donde residen los datos de los ciudadanos, así como habilitar un canal en el firewall municipal que permita el acceso. Los datos serán accedidos y viajarán a la plataforma cloud situada en Italia aunque en esta no se almacenarán.

I

Dada la complejidad del proyecto y las implicaciones que en materia de protección de datos presenta, debe hacerse una referencia previa a diversos conceptos propios de esta materia o en directa relación con ella, que deben ser tomados en cuenta por el consultante en relación con los diferentes tratamientos de datos personales que pretende llevar a cabo.

Con carácter general, debe indicarse que los artículos 1 y 2 de la Ley Orgánica 15/1999, extienden su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento de sus datos de carácter personal, siendo

definidos éstos en el artículo 3.a) de la citada Ley como "*cualquier información concerniente a personas físicas identificadas o identificables.*"

El Grupo de trabajo del artículo 29, órgano consultivo independiente de la Unión Europea sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo de la Directiva 95/46/CE, 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, en su Dictamen 4/2007 sobre el concepto de datos personales, tras poner de manifiesto que la Directiva maneja un concepto lato de datos personales, analiza los elementos de dicha definición, señalando respecto a la expresión "toda información" que "*Desde el punto de vista del contenido de la información, el concepto de datos personales incluye todos aquellos datos que proporcionan información cualquiera que sea la clase de ésta. Por supuesto esto incluye la información personal considerada «datos sensibles» en el artículo 8 de la Directiva a causa de su naturaleza particularmente delicada, pero también otras categorías más generales de información. El término «datos personales» comprende la información relativa a la vida privada y familiar del individuo stricto sensu, pero también la información sobre cualquier tipo de activad desarrollada por una persona, como la referida a sus relaciones laborales o a su actividad económica o social. El concepto de «datos personales» abarca, por lo tanto, información sobre las personas, con independencia de su posición o capacidad (como consumidor, paciente, trabajador por cuenta ajena, cliente, etc.).*"

El artículo 5.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, concreta la definición de dato personal especificando que constituye un dato de carácter personal *"Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables."*

Por otra parte, la definición contenida en el artículo 3.a de la Ley Orgánica 15/1999 se complementa con la de persona identificable, a la que se refiere el artículo 5.1.o) de su Reglamento de desarrollo, que dispone que lo será "*toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados".*

Ambas definiciones tienen su origen en lo establecido en la Directiva 95/46/CE, cuyo artículo 3 califica como dato personal "*toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".*

Para determinar que se entiende por persona identificada o identificable, cabe acudir a lo señalado, en el aludido Dictamen 4/2007 del Grupo de Trabajo del artículo 29. Dicho dictamen analiza los términos contenidos en la definición aportada por la Directiva señalando respecto al concepto de persona identificada o identificable lo siguiente:

> "La Directiva requiere que la información se refiera a una persona física «identificada o identificable». Ello suscita las siguientes consideraciones. De modo general, se puede considerar «identificada» a una persona física cuando, dentro de un grupo de personas, se la «distingue» de todos los demás miembros del grupo. Por consiguiente, la persona física es «identificable» cuando, aunque no se la haya identificado todavía, sea posible hacerlo (que es el significado del sufijo «ble»). Así pues, esta segunda alternativa es, en la práctica, la condición

suficiente para considerar que la información entra en el ámbito de aplicación del tercer componente. La identificación se logra normalmente a través de datos concretos que podemos llamar «identificadores» y que tienen una relación privilegiada y muy cercana con una determinada persona. Cabe citar como ejemplos su apariencia exterior, es decir su altura, el color del cabello, la ropa, etc. o una cualidad de la persona que no puede percibirse inmediatamente, como su profesión, el cargo que ocupa, su nombre, etc. La Directiva menciona esos «identificadores» en la definición de «datos personales» del artículo 2 cuando establece que «*se declarará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social*».

En lo que respecta a los términos "directa" o "indirectamente" identificable continúa señalando el Grupo de Trabajo del artículo 29 que:

"Esta idea se aclara aún más en los comentarios a los artículos de la propuesta modificada de la Comisión, en donde se afirma que *«una persona puede ser identificada directamente por su nombre y apellidos o indirectamente por un número de teléfono, la matrícula de un coche, un número de seguridad social, un número de pasaporte o por una combinación de criterios significativos (edad, empleo, domicilio, etc.), que haga posible su identificación al estrecharse el grupo al que pertenece."*

Los términos de esta declaración indican claramente que el que determinados identificadores se consideren suficientes para lograr la identificación es algo que depende del contexto de la situación de que se trate. Un apellido muy común no bastará para identificar a una persona - es decir, para aislarla – dentro del conjunto de la población de un país, mientras que es probable que permita la identificación de un alumno

dentro de una clase. Incluso una información auxiliar, como, por ejemplo, «el hombre que lleva un traje negro», puede identificar a alguno de los transeúntes que esperan en un semáforo. Así pues, el que se identifique o no a la persona a la que se refiere una información depende de las circunstancias concretas del caso.

Por su parte, cuando hablamos de «indirectamente» identificadas o identificables, nos estamos refiriendo en general al fenómeno de las «combinaciones únicas», sean éstas pequeñas o grandes. En los casos en que, a primera vista, los identificadores disponibles no permiten singularizar a una persona determinada, ésta aún puede ser «identificable», porque esa información combinada con otros datos (tanto si el responsable de su tratamiento tiene conocimiento de ellos como si no) permitirá distinguir a esa persona de otras. Aquí es donde la Directiva se refiere a «uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social». Algunas de esas características son tan únicas que permiten identificar a una persona sin esfuerzo (el «actual Presidente del Gobierno de España »), pero una combinación de detalles pertenecientes a distintas categorías (edad, origen regional, etc.) también puede ser lo bastante concluyente en algunas circunstancias, en especial si se tiene acceso a información adicional de determinado tipo. Este fenómeno ha sido estudiado ampliamente por los estadísticos, siempre dispuestos a evitar cualquier quebrantamiento de la confidencialidad.”

Estas definiciones deben ponerse en relación con lo que se viene denominando “datos abiertos”, en tanto que el proyecto objeto de consulta hace referencia a la utilización de los mismos, así como a la de datos personales obrantes en los archivos de las Administraciones Públicas, a fin de delimitar en qué supuestos y con qué condiciones pueden los datos personales obrantes en

los archivos de las Administraciones públicas considerarse como datos abiertos o susceptibles de reutilización

En este sentido, la Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público, planteaba como objetivo que la información del sector público que estuviese a disposición del público con arreglo a la legislación nacional pudiera ser reutilizada con fines comerciales o no comerciales. Desde el punto de vista de la normativa de protección de datos, el considerando 21 de la mencionada Directiva 2003/98/CE dispone que "*La presente Directiva se debe incorporar al Derecho interno y aplicar de forma que se cumplan plenamente los principios relativos a la protección de los datos personales, de conformidad con la 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".*

Este principio se reitera en la reforma operada por la Directiva 2013/37/UE, del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por la que se modifica la Directiva 2003/98/CE, cuyo considerando 34 señala que "*La presente Directiva respeta los derechos fundamentales y observa los principios reconocidos, en particular, por la Carta de los Derechos Fundamentales de la Unión Europea, incluidos la protección de los datos de carácter personal (artículo 8) y el derecho a la propiedad (artículo 17). Nada de lo contenido en la presente Directiva debe interpretarse o aplicarse en un sentido que no sea acorde con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales"*. En particular, en lo que al derecho fundamental a la protección de datos se refiere, el considerando 11 de la Directiva añade, con mayor precisión que la contenida en la Primera Directiva, que "*la presente Directiva debe incorporarse al Derecho interno y aplicarse de forma que se cumplan plenamente los principios relativos a la*

protección de los datos personales, de conformidad con la 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. En particular, conviene señalar que, con arreglo a dicha Directiva, los Estados miembros deben determinar las condiciones en las que sea legal el tratamiento de datos personales. Además, uno de los principios de dicha Directiva consiste en que los datos personales no deben ser tratados posteriormente a una recogida de un modo que sea incompatible con los objetivos determinados, explícitos y legítimos para los que dichos datos fueron recogidos".

El texto actualmente vigente de la Directiva 2003/98 incide aún en mayor medida en el necesario respeto a las normas de protección de datos, por cuanto el nuevo artículo 1.2 c *quater* excluye del ámbito de aplicación de la misma:

-Los documentos a los que no pueda accederse en virtud de regímenes de acceso por motivos de protección de los datos personales.

-Los documentos cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de los datos personales

- Las partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización se haya definido por ley como incompatible con la legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales.

Respecto de las limitaciones a la reutilización derivadas de este precepto, debe tenerse en cuenta lo señalado por el aludido Grupo de Trabajo del artículo 29 en su Dictamen 06/2013 sobre datos abiertos y reutilización de la información del sector público (ISP), adoptado el 5 de junio de 2013, en que, como primera conclusión, se pone de manifiesto que "el «principio de reutilización» no es automático cuando está en juego el derecho a la protección de los datos personales, y no anula las disposiciones aplicables de la normativa

sobre protección de datos. Cuando los documentos en poder de los organismos del sector público contienen datos personales, su reutilización está incluida en el ámbito de aplicación de la Directiva 95/46/CE y, por tanto, está sujeta a la normativa sobre protección de datos aplicable", añadiendo así que "en los casos en que la reutilización incluye datos personales, el organismo del sector público no puede invocar sistemáticamente la necesidad de cumplir con la Directiva ISP como razón legítima para facilitar datos para su reutilización", de modo que que, "desde la perspectiva de quien reutiliza los datos, la Directiva ISP en sí misma no crea un motivo legítimo para el tratamiento".

A continuación, el apartado V del Dictamen se dedica específicamente al análisis de las limitaciones al principio de reutilización vinculadas a la aplicación de las normas reguladoras del derecho fundamental a la protección de datos de carácter personal, que resultan especialmente de interés en tanto que el artículo 3.j de la Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público reproduce lo establecido en la el artículo 1.2.c) quater de la Directiva 2003/98. Dispone el aludido artículo 3.j *" La presente Ley no será aplicable a los siguientes documentos que obren en las Administraciones y organismos del sector público previstos en el artículo 2: (…) j) Los documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de los datos personales, de conformidad con la normativa vigente y las partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización se haya definido por ley como incompatible con la legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales."*

El Dictamen diferencia tres límites a la reutilización derivados de la aplicación de las normas de protección de datos, vinculados a su vez con lo establecido en los distintos Estados Miembros en relación con el acceso a la información del sector público:

El primer supuesto se refiere a los supuestos en que está prohibido el acceso en aplicación de las normas de protección de datos de carácter personal, recordando la doctrina establecida por el Tribunal de Justicia de la Unión en diversas sentencias y vinculando esta prohibición general a lo dispuesto en la normativa de los distintos Estados Miembros en relación con el acceso a la información pública. Así, se hace referencia a las sentencias del TJ de 20 de mayo de 2003 (Asunto Österreichischer Rundfunk) y de 9 de noviembre de 2010 (Asunto Volker und Markus Schecke), que coinciden en establecer que el mero acceso a la información pública, como restricción a un derecho fundamental, el de protección de datos de carácter personal, debe cumplir los requisitos exigidos para ello por el Convenio Europeo de Derechos Humanos y la jurisprudencia del Tribunal Europeo de Derechos Humanos; es decir, estar prevista en una Ley, perseguir un objetivo legítimo y constituir una medida proporcional en una sociedad democrática para obtener ese objetivo. En el mismo sentido, cabe hacer referencia a la Sentencia de 29 de junio de 2010 (asunto Bavarian Lager).

Una segunda categoría de supuestos, según el Dictamen, incluiría aquellos documentos cuyo acceso esté limitado como consecuencia de la aplicación de las normas de protección de datos, que imponen alguna exigencia adicional para el acceso, como por ejemplo la acreditación de un interés legítimo por parte del solicitante, tal y como ocurriría, por ejemplo, en España para el acceso al Registro de la Propiedad, en los términos establecidos en la Ley Hipotecaria, que exige la concurrencia del mencionado interés en el solicitante de la publicidad registral.

Por último, el Dictamen se refiere a una tercera categoría de documentos del sector público en que el régimen aplicable puede resultar más complejo, cuales son aquéllos que en principio pueden ser susceptibles de acceso conforme a la normativa de acceso a la información pública, pero cuya

reutilización se encuentra limitada por resultar incompatible con la legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales. A tal efecto, el Dictamen se refiere a una serie de ejemplos que pudieran ser aplicables y concluye lo siguiente:

> *"En todos los casos, el organismo del sector público interesado debe realizar una cuidadosa evaluación de impacto sobre la protección de datos para decidir si pueden facilitarse los datos para su reutilización en la Directiva ISP y, de ser así, si la legislación sobre protección de datos requiere condiciones específicas y salvaguardias. El «principio de reutilización» no es automático, y no puede tener prioridad sobre las disposiciones aplicables de la normativa de protección de datos.*
>
> *Esta evaluación detallada es tanto más importante dado que, en virtud de la Directiva ISP, el organismo del sector público, en principio, no debe analizar quien es el solicitante concreto que pide acceso para la reutilización. De conformidad con el artículo 10 (No discriminación), «las condiciones que se apliquen para la reutilización de un documento no deberán ser discriminatorias para categorías comparables de reutilización». Asimismo, conformidad con el artículo 11 (Prohibición de los acuerdos exclusivos), «la reutilización de documentos estará abierta a todos los agentes potenciales del mercado... Los contratos o acuerdos de otro tipo entre los organismos del sector público que conserven los documentos y los terceros no otorgarán derechos exclusivos.»*
>
> *Por consiguiente, al decidir si autorizan o no la reutilización, los organismos del sector público deben tener en cuenta la compatibilidad de permitir la reutilización en virtud de una licencia abierta no solo al solicitante, sino también a cualquiera que pida los datos. Esto requiere un alto nivel de confianza en que ninguno de los reutilizadores*

potenciales podrá hacer un uso indebido de los datos personales facilitados.

La Directiva ISP no excluye que los términos y condiciones puedan autorizar el tratamiento solo para fines específicos. La cuestión que se plantea al organismo del sector público es por tanto si la reutilización, por cualquier «posible agente del mercado», a estos efectos, es compatible con las finalidades previstas por el organismo del sector público. La potencial reutilización por parte de las entidades financieras de la información sobre el pago de impuestos, por ejemplo, para fines de información crediticia, es pertinente ya que siguen siendo un potencial reutilizador, según el criterio de «cualquier persona». Por tanto, para resolver los problemas de protección de datos y en particular para garantizar el cumplimiento del principio de limitación de la finalidad, el organismo del sector público (o el legislador) deberá poder limitar, en su caso, las finalidades de la reutilización."

En el presente proyecto se hace referencia a la utilización de los datos contenidos en el Padrón del Ayuntamiento consultante. El régimen de dicho fichero se contiene en la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local, cuyo artículo 16.1 dispone que "1. *El Padrón municipal es el registro administrativo donde constan los vecinos de un municipio. Sus datos constituyen prueba de la residencia en el municipio y del domicilio habitual en el mismo. Las certificaciones que de dichos datos se expidan tendrán carácter de documento público y fehaciente para todos los efectos administrativos*." Por su parte el número 3 de dicho artículo fija los supuestos en que es posible la comunicación de datos contenidos en el mismo al establecer que "*Los datos del Padrón Municipal se cederán a otras Administraciones públicas que lo soliciten sin consentimiento previo al afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos*

relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública y en las leyes de estadística de las comunidades autónomas con competencia en la materia."

Esta Agencia ha examinado la interpretación que debe darse a dicho precepto en numerosos informes, concluyendo que el concepto de Administración Pública se corresponde con el señalado en los artículos 2.1 de la Ley 30/1992, de 26 de noviembre, de Régimen jurídico de las Administraciones públicas y del Procedimiento Administrativo común (en los mismos términos los artículo 2.3 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Publicas y 2.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público) y el artículo 1.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, por lo que la referencia a las Administraciones Públicas que realiza el artículo 16.3 de la 7/1985, de 2 de abril, de Bases del Régimen Local solamente puede ser entendida como referencia a las Administraciones Públicas españolas y dentro del sector público a las entidades mencionadas en dichos preceptos.

Asimismo, esta Agencia ha venido señalando que para que la comunicación de datos personales contenidos en el Padrón municipal prevista en el artículo 16.3 de la Ley 7/1985 sea conforme a lo previsto en la normativa de protección de datos debe realizarse en el marco de las competencias legalmente atribuidas a la Administración Pública cesionaria y venir amparada en una norma con rango de Ley tal y como exige el artículo 11.2.a) de la Ley Orgánica 15/1999 cuando no exista consentimiento del interesado. Deberá asimismo respetar el principio de proporcionalidad recogido en el artículo 4 de la Ley Orgánica 15/1999, por lo que no cabe una cesión masiva de los datos contenidos en dicho Padrón. Asimismo, esta Agencia ha interpretado que la expresión «datos del Padrón municipal» que se emplea en el artículo 16.3 de la

Ley de Bases de Régimen Local se refiere únicamente a los datos que en sentido propio sirven para atender a la finalidad a que se destina el Padrón municipal: la determinación del domicilio o residencia habitual de los ciudadanos, la atribución de la condición de vecino, la determinación de la población del municipio y la acreditación de la residencia y domicilio. Por ello, cualquier comunicación o cesión de los datos del Padrón deberá fundarse en la necesidad por la Administración cesionaria, en el ejercicio de sus competencias, de conocer el dato del domicilio de la persona afectada, dado que del artículo 4.2 de la Ley se deriva la imposibilidad del tratamiento de los datos para fines diferentes de los que motivaron su recogida, salvo que así lo consienta el afectado o la Ley lo prescriba.

Por consiguiente, el régimen del padrón municipal quedaría incluido en aquéllos a que hace referencia el artículo 3.j de la Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, por lo que no puede considerarse que los datos contenidos en el mismo son susceptibles de reutilización, de este modo será preciso que cualquier comunicación de los datos personales en él contenidos sea conforme a lo establecido en la Ley Orgánica 15/1999.

No obstante, la identificación de las personas puede evitarse mediante un proceso de disociación, la Ley Orgánica 15/1999 describe éste en su artículo 3 f) como *"Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable*" Debe a este respecto, tomarse en consideración lo indicado por el grupo de Trabajo del artículo 29 en el aludido Dictamen 6/2013 en cuanto a la posibilidad de facilitar datos contenidos en los ficheros de las Administraciones Públicas eliminando datos personales, que a continuación se reproduce parcialmente:

"Hasta la fecha, las iniciativas sobre reutilización de la ISP lanzadas por los organismos del sector público a través de «portales de datos abiertos» u otras plataformas han tenido generalmente como objetivo facilitar datos agregados y anonimizados para su reutilización, en vez de datos personales como tales. Este planteamiento es más seguro y debe fomentarse.

Las leyes de protección de datos no suelen permitir que los organismos del sector público publiquen datos personales recogidos para otro fin, generalmente administrativo. Por tanto, en estos casos, su reutilización como parte de las iniciativas de reutilización de la ISP tampoco es posible. En vez de datos personales, se facilitan y deberían facilitarse (en principio) datos estadísticos derivados de los datos personales. Esta es la solución más eficaz para minimizar el riesgo de revelación inadvertida de datos personales. Estas series de datos agregados y anonimizados no deberán permitir la reidentificación de las personas y, por tanto, no deben contener datos personales.

Decidir el nivel de agregación adecuado y las técnicas específicas de anonimización que deben utilizarse es una tarea difícil. Si la agregación y la anonimización no se hacen de manera eficaz, esto entraña el riesgo de que los individuos puedan ser reidentificados a partir de estos conjuntos de datos. Por tanto, la legislación sobre protección de datos tiene un papel importante que desempeñar a la hora de contribuir a determinar el umbral a partir del cual es «seguro» comunicar datos agregados y anonimizados como parte de una iniciativa de la ISP.

La Directiva 95/46/CE establece un alto nivel para el umbral de anonimización. En el presente documento, el término «anonimización» se refiere a los datos que ya no pueden considerarse datos personales de conformidad con el artículo 2, letra a), de la Directiva 95/46/CE. El artículo

2, apartado a) define los «datos personales» como «toda información sobre una persona física identificada o identificable (el "interesado")». Se considerará identificable «toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social»

.

El considerando 26 de la Directiva 95/46/CE es también pertinente y dispone además que, con el fin de «determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona».

Hay que señalar que ello establece un umbral elevado, como se expondrá más adelante en el presente Dictamen. Salvo que los datos puedan anonimizarse para alcanzar este umbral, sigue siendo aplicable la legislación sobre protección de datos. Esto significa, entre otras cosas, que a menos que se alcance el umbral, la publicación de la información (y cualquier uso posterior) debe ser «compatible» con las finalidades iniciales de la recogida de datos con arreglo al artículo 6, apartado 1, letra b), de la Directiva 95/46/CE. Además, también deberá existir una base jurídica adecuada para el tratamiento en virtud del artículo 7, apartado 2, letras a) a f), de la Directiva 95/46/CE (por ejemplo, el consentimiento, o necesidad de cumplir la ley). En cambio, si los datos han sido anonimizados en el sentido del artículo 2, letra a), y del considerando 26 de la Directiva 95/46/CE, las normas sobre protección de datos dejarán de ser aplicables y los reutilizadores podrán reutilizar los datos sin estas limitaciones Una vez más, es preciso hacer hincapié en el hecho de que «datos anonimizados», según el presente Dictamen, son datos que ya no se consideran personales. Los datos anonimizados deben distinguirse, en particular, de los datos que han sido manipulados utilizando diversas

técnicas para mitigar los riesgos de reidentificación de los individuos en cuestión, pero que no han alcanzado el umbral establecido en el artículo 2, letra a), y en el considerando 26 de la Directiva 95/46/CE24. En muchos supuestos, estas técnicas solo resultan adecuadas para una divulgación limitada a efectos de su reutilización por terceros, pero no para su plena divulgación y reutilización con licencia abierta.

Es también importante hacer hincapié en que una vez que los datos se publican para su reutilización, no habrá control alguno sobre quién puede acceder a ellos. La probabilidad de que «cualquier otra persona» tenga los medios y los utilice para reidentificar a los interesados aumentará considerablemente. Por tanto, y con independencia de la interpretación del considerando 26 en otros contextos, cuando se trata de facilitar datos para su reutilización en virtud de la Directiva ISP, el Grupo de trabajo del artículo 29 desea dejar absolutamente claro que debe tenerse el mayor cuidado en garantizar que los conjuntos de datos facilitados no incluyan datos que puedan ser reidentificados por medios que puedan ser razonablemente utilizados por cualquier persona, incluidos los reutilizadores potenciales, pero también por otras partes que puedan tener interés en obtener los datos, incluidos los servicios con funciones coercitivas.

La anonimización es cada vez más difícil de lograr con el avance de las modernas tecnologías informáticas y la disponibilidad de la información de forma ubicua. La reidentificación de las personas es cada vez más común y representa una amenaza en la actualidad. En la práctica, existe una importante zona gris, en la que el responsable del tratamiento de datos puede creer que un conjunto de datos está anonimizado, pero un tercero puede ser capaz de identificar al menos a algunas personas a partir de estos datos, por ejemplo, utilizando otros datos públicos o cualquier otra información de que disponga.

> Uno de los principales factores de riesgo es el aumento de la cantidad de datos en línea y fuera de línea, tanto a disposición del público como en manos de organizaciones empresariales, que pueden utilizarse para trazar el perfil de las personas con fines de publicidad comportamental y para un abanico creciente de otros fines. Al cotejarse con la realidad de los «grandes datos» de que ya disponen estas organizaciones, la ISP derivada de los datos personales y facilitada para su reutilización podría aumentar la probabilidad de que los particulares puedan ser identificados o de que sus perfiles pueden verse enriquecidos, a menudo sin que las personas sean conscientes de que esté ocurriendo."

Por consiguiente, la comunicación de los datos obrantes en el Padrón fuera de los supuestos permitidos por la Ley o en que exista un consentimiento de los afectados solo será posible si los datos se encuentran anonimizados. En este sentido la Ley Orgánica 15/1999 describe el proceso de disociación en su artículo 3.f como *"Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable"*

Resulta de especial interés en lo que respecta a la disociación de los datos lo indicado por el Grupo de Trabajo del artículo 29 en su Dictamen 5/2014 sobre técnicas de anonimización, en el que se ponía de manifiesto que:

"El Grupo de Trabajo examinó el concepto de «datos personales» en el Dictamen 4/2007 sobre datos personales, en el que se centra en los elementos componentes de la definición del artículo 2, letra a), de la Directiva 95/46/CE, entre ellos la referencia a una persona física «identificada o identificable». En este contexto, el Grupo de Trabajo llegó a la conclusión de que «los datos

anonimizados serían, por tanto, datos anónimos que antes hacían referencia a una persona identificable, pero que ahora ya no admiten identificación».

Por consiguiente, el Grupo de Trabajo ya ha aclarado que la Directiva propone la razonabilidad de los medios usados («el conjunto de los medios que puedan ser razonablemente utilizados») como criterio para evaluar si el tratamiento de anonimización es suficientemente sólido, es decir, si la identificación es «razonablemente» imposible. Afectan directamente a la identificabilidad el contexto y las circunstancias particulares de cada caso.

(…) Una solución de anonimización eficaz impide a todos singularizar a una persona en un conjunto de datos, vincular dos registros en un conjunto de datos (o dos registros pertenecientes a conjuntos diferentes) e inferir cualquier tipo de información a partir de dicho conjunto. En definitiva, como norma general, no basta con eliminar los elementos que pueden servir para identificar directamente a una persona para garantizar que ya no se puede identificar al interesado. Con frecuencia habrá que tomar medidas adicionales para evitar dicha identificación, las cuales dependerán una vez más del contexto y de los fines del tratamiento de que van a ser objeto los datos."

Recuerda asimismo dicho Dictamen que "Es importante dejar claro que el concepto de «identificación» no conlleva únicamente la posibilidad de recuperar el nombre o la dirección de una persona, sino que incluye también la identificabilidad potencial por singularización, vinculabilidad o inferencia. Es más, a efectos legales es irrelevante la intención del responsable del tratamiento o del destinatario. Mientras los datos sean identificables, se aplica la legislación sobre protección de datos."

Estos aspectos deben tenerse en cuenta respecto de los tratamientos y cesiones de datos a realizar por el Ayuntamiento en relación con el concepto de open data, en particular respecto de los datos que en tal calidad pudiera

publicar y que sean resultado de un proceso de disociación de los datos personales obrantes en los ficheros municipales (sea el Padrón o cualquier otro que contenga datos personales), recordando que no es suficiente con eliminar los elementos que identifican directamente a la persona (nombre, dirección) sino que es preciso una agregación suficiente de los datos para evitar la re-identificación de las personas cuyos datos, aunque separados de los que le identifican directamente, se hacen públicos.

II

De lo señalado en la documentación aportada se desprende que el proyecto piloto dará lugar a diversos tratamientos y cesiones de datos personales obrantes en el Padrón municipal. A este respecto debe recordarse que constituye un tratamiento de datos, conforme a lo establecido en el artículo 3.c de la Ley Orgánica 15/1999, las *"operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."* Por consiguiente, la realización de cualquiera de estas operaciones estará sujeta a la normativa de protección de datos. Asimismo su artículo el artículo 3 i) define la cesión de datos como "*toda revelación de datos realizada a una persona distinta del interesado"* por lo que tanto la comunicación o difusión de los datos personales contenidos en el Padrón, como cualquier acceso a las bases del mismo constituirá una cesión de datos personales.

Debe igualmente recordarse que el Ayuntamiento consultante tiene la condición de responsable del Padrón de su municipio, tal y como éste se configura en la Ley Orgánica 15/1999, esto es, como "*persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la*

finalidad, contenido y uso del tratamiento" y al que le corresponde asumir la responsabilidad del cumplimiento de las normas de protección de datos.

Siendo el Ayuntamiento responsable del fichero constituido por las diferentes bases de datos que conforman el Padrón Municipal, entre sus responsabilidades se encuentran la de custodiar los datos de modo que no sean comunicados a terceros carentes de legitimación ni accedidos indebidamente.

En lo que respecta a la legitimación para el correspondiente tratamiento o cesión de datos, ya se han señalado los supuestos en que la propia Ley de Bases de régimen Local legitima la comunicación de datos del Padrón municipal sin consentimiento de los interesados. De este modo, fuera de estos supuestos u otros que puedan venir previstos en una Ley, la comunicación de datos a Administraciones Públicas de otros países o a empresas privadas exige el consentimiento del interesado. Dispone así el artículo 11 de la Ley Orgánica 15/1999 que "*Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado."*

Dicho consentimiento debe quedar acreditado con carácter previo a la cesión de datos que se efectúe, siendo al responsable del fichero conforme a lo establecido en el artículo 12 del Reglamento de desarrollo de la Ley Orgánica a quien corresponde probar la existencia del mismo.

Debe tenerse en cuenta, además que dicho consentimiento deberá reunir las características señaladas en el artículo 3 h) de la misma norma según el cual el consentimiento deberá ser "libre, inequívoco, específico e informado". Esta Agencia ha venido describiendo en sus informes dichas características de manera que se entiende por consentimiento libre aquel que

ha sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil. El consentimiento específico viene referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, tal y como impone el artículo 4.2 de la Ley Orgánica 15/1999. Para que pueda hablarse de consentimiento inequívoco se exige la realización de una acción u omisión que implique la existencia del consentimiento, acción que, en el presente supuesto, vendría constituida por la actuación del interesado solicitando la emisión del correspondiente certificado, para dicho tratamiento de datos y, en su caso, la comunicación a uno o varios terceros sean estos otra Administración Pública española o extranjera o a una empresa.

En cuanto al requisito de la información, supone que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que se efectúa. Dispone a este respecto el artículo 5 de la Ley Orgánica 15/1999 que *"los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".*

Asimismo, debe recordarse que el consentimiento así prestado siempre es revocable conforme a los artículos 6.3 y 11.4 de la Ley Orgánica 15/1999, pudiendo el interesado exigir el cese en el tratamiento de sus datos mediante su pura y simple manifestación de voluntad.

Asimismo, la comunicación de datos que se lleve a cabo debe respetar el principio de proporcionalidad, respecto del cual dispone el artículo 4.1 de la Ley orgánica 15/1999 "*Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinados, explícitas y legítimas para las que se hayan obtenido*." De este modo el consentimiento habilita a quien lo ha obtenido a conocer exclusivamente aquellos datos que sean precisos para la finalidad para la que fue recabado. A título de ejemplo, si la finalidad es emitir un certificado de residencia, resulta desproporcionado acceder al dato relativo al nivel de estudios que igualmente figurará en el Padrón, y que no resulta necesario para dicha emisión.

Debe aquí hacerse una referencia a la figura del encargado del tratamiento. Dicha figura viene regulada en el artículo 12 de la Ley Orgánica 15/1999 según el cual *"No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento*." El encargado del tratamiento responde a la necesidad de dar respuesta a fenómenos como la externalización de servicios por parte de las empresas y otras entidades, de manera que en aquellos supuestos en que el responsable del tratamiento encomiende a un tercero la prestación de un servicio que requiera el acceso a datos de carácter personal por éste, dicho acceso no pueda considerarse como una cesión de datos.

El Reglamento de desarrollo de la Ley Orgánica 15/1999, precisa en su artículo 20 que "*El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente capítulo.*

El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado."

Por tanto, para determinar si nos encontramos en presencia de un encargado del tratamiento deberá analizarse si su actividad se encuentra limitada a la mera prestación de un servicio al responsable, sin generarse ningún vínculo entre el afectado y quien realiza dicha actividad. De este modo no cabe considerar como encargado del tratamiento a una empresa o entidad que además de prestar un servicio al Ayuntamiento (por ejemplo el servicio de cloud o servicios técnicos o de desarrollo de programas) utilice los datos para sus propios fines prestando los servicios añadidos a que la consulta se refiere, en tanto se establece una relación entre ambos que impide la consideración de dicha relación como la propia de un encargado del tratamiento.

Asimismo, en el marco del derecho español, para que la relación entre responsable y encargado del tratamiento pueda darse y se ajuste a la Ley, es preciso que se cumplan los requisitos expresados en el artículo 12 de la Ley Orgánica 15/1999, considerando los siguientes aspectos:

En primer lugar, es preciso que el acceso a los datos por el tercero se efectúe con la exclusiva finalidad de prestar un servicio al responsable del fichero, y que dicha relación de servicios se encuentre contractualmente establecida. En lo que atañe a los requisitos formales de este tipo de contratos, el artículo 12.2 de la Ley Orgánica 15/1999, impone que "*la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del*

responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas".

El hecho de que la relación derivada del contrato sea la existente entre un responsable y un encargado del tratamiento implicará que al término de la relación sea aplicable lo establecido en el artículo 12.3 de la Ley Orgánica 15/1999, de forma que *"una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".*

El incumplimiento de esta previsión llevará aparejada la consecuencia, prevista en el artículo 12.4 de la citada Ley, de que "*En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente".*

Por último, en cuanto a las medidas de seguridad que hayan de ser adoptadas por quienes realicen trabajos de tratamiento de datos por cuenta de tercero, habrán de ser, en principio, las mismas que las impuestas al responsable del fichero, tal y como se desprende de lo previsto en los artículo 9 y 12.2 de la Ley Orgánica 15/1999.

III

Teniendo en cuenta lo anteriormente señalado, cabría considerar que la empresa que presta los servicios de desarrollo de los microservicios y servicios complejos podría tener la condición de encargado del tratamiento del Ayuntamiento, siempre que se dé cumplimiento a los requisitos del artículo 12

de la Ley Orgánica 15/1999 y, tal y como se ha señalado, no utilice los datos personales para fines propios (entre los que se encontrarían la prestación de los denominados servicios añadidos) lo que resultaría incompatible con la figura de encargado del tratamiento. De la misma manera la entidad que presta servicios de cloud computing cumpliendo tales requisitos sería considerada como encargada del tratamiento.

No obstante, en el entorno limitado del proyecto objeto de consulta podría configurarse como cesiones de datos las comunicaciones de datos que se efectúen tanto a las empresas que formen parte del consorcio, como, en su caso, a las demás Administraciones piloto que pudieran tener algún tipo de acceso a los datos (aunque sea meramente una visualización de los datos con motivo de las pruebas o demostraciones de funcionamiento del proyecto). Ello siempre y cuando todas ellas tengan acceso únicamente a los datos de quienes hayan prestado su consentimiento para la comunicación de los mismos, se garantice que los datos no van a ser utilizados por ninguno de los cesionarios con fines distintos a los propios del proyecto y exista una cláusula de confidencialidad.

Asimismo, en todo caso, deberá darse cumplimiento al principio de conservación de los datos recogido en el artículo 4.5 de la Ley Orgánica 15/1999 según el cual que "*Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados".* Ello determina que los datos personales recogidos por los participantes en el proyecto, no podrán mantenerse indefinidamente en sus ficheros, debiendo cancelarse una vez que dejen de ser necesarios para los fines del mismo. En este sentido, los proyectos examinados por esta Agencia vienen a señalar un plazo para proceder a su destrucción, generalmente de un año después de la conclusión del proyecto, entendiendo que en tal momento dejarán de ser precisos para la finalidad para la que fueron originalmente recabados.

Por último, en lo que respecta a los participantes en el proyecto no establecidos en un Estado miembro, debe recordarse que la transmisión de datos a entidades situadas fuera del Espacio Económico Europeo constituirá una transferencia internacional de datos, tal y como establece el artículo 5.1 s) del Reglamento de desarrollo de la Ley Orgánica 15/1999, al definir estas como el "*tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español".* Deberá así estarse al régimen regulado en los artículos 33 y 34 de la Ley Orgánica 15/1999 y en el Titulo VI de su reglamento de desarrollo.

Dispone a este respecto el artículo 33.1 de la Ley Orgánica 15/1999 que "*no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas*".

El artículo 33.2 de la Ley Orgánica 15/1999 establece los criterios para determinar el carácter adecuado de protección al disponer que "*el carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos de finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la*

Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países". En este sentido cabe recordar que la Comisión de la Unión Europea ha adoptado decisiones en las que se ha considerado que existe un nivel adecuado de protección en Estados tales como Suiza, Argentina, Uruguay, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Canadá respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos y Nueva Zelanda. La decisión en la que se consideraba que existía un nivel de protección adecuado respecto de las entidades estadounidenses adheridas a los «principios de Puerto Seguro ha sido anulada por la Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015, .asunto C-362/14. Shrems v Data Protection Commissioner.

En el presente supuesto, en que uno de los países participantes en el proyecto, no forma parte del espacio económico europeo ni existe una decisión en la que se considere que existe en el mismo un nivel adecuado de protección, sería preciso solicitar dicha autorización. No obstante, teniendo nuevamente en cuenta el marco en el que se produce la misma limitado a los participantes en el proyecto y el hecho de que se ha solicitado a los interesados el consentimiento para la cesión de sus datos mencionando expresamente a los cesionarios, cabe considerar que resulta de aplicación la excepción a la obligación obtener tal autorización contenida en el artículo 34,e) de la Ley Orgánica 15/1999 relativa a que el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

IV

En lo que respecta a un posible desarrollo futuro, entendiendo por tal el relativo al desarrollo de servicios innovadores basados en consultas al Padrón Municipal, u otros ficheros públicos, enriquecido con información publicada

proveniente del portal de datos abiertos, requeriría conocer con más detalle cómo se van a prestar dichos servicios, no obstante cabe apuntar algunas de las cuestiones que en principio plantean la prestación conjunta de servicios públicos y privados:

La primera de ellas hace referencia al cumplimiento de los principios y obligaciones regulados en la Ley Orgánica 15/1999.

Debe así recordarse que el artículo 4.2 de la Ley Orgánica 15/1999 recoge el principio de finalidad disponiendo que *"Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos".* Debe, en este sentido recordarse en cuanto a la interpretación del término "incompatible" que la Audiencia Nacional ha venido a concluir que la Ley Orgánica 15/1999 utiliza la expresión "*finalidades incompatibles"* como sinónimo de "*finalidades distintas".*

El principio de finalidad recogido en el artículo 4 de la Ley Orgánica 15/1999 debe además, aplicarse de modo especialmente riguroso en el ámbito de la Administración pública, toda vez que los datos se recogen por ésta en virtud de la excepción a la necesidad de consentimiento del interesado prevista en el citado artículo 6.2 de la misma Ley, constituyendo dicha excepción una limitación al poder de disposición y control sobre los datos personales en que consiste el derecho fundamental a la protección de datos.

Así, en el marco de las Administraciones Públicas debe recordarse que la finalidad que justifica el tratamiento de datos personales es el ejercicio de la competencia legalmente atribuida al órgano responsable del tratamiento. Así se desprende de lo establecido en el artículo 6.2 de la Ley Orgánica 15/1999, que justifica el tratamiento de los datos por las administraciones públicas en el ejercicio de las competencias a las mismas atribuidas, por lo que su utilización para finalidades distintas solo es posible cuando así está establecido en una Ley o el interesado lo consiente.

De otra parte, la Administración no puede imponer a los interesados que solicitan un servicio público que dicha prestación esté unida a un servicio añadido de carácter comercial que facilitan una o varias empresas, ni tampoco cabe que la Administración publicite tales servicios añadidos más allá de indicar a los ciudadanos que tales servicios existen y donde pueden acceder a ellos.

La posible comunicación de datos a las empresas que prestan un servicio añadido, además de la necesidad de consentimiento del interesado que debe requerir la Administración que cede los datos con carácter previo a dicha cesión, exigiría una valoración del principio de proporcionalidad en cada caso respecto a los datos a comunicar. Cabe así recordar que solamente se podrán ceder, aquellos datos "adecuados, pertinentes y no excesivos" para la finalidad "determinada, explícita y legítima" de que se trate. Así por ejemplo si el servicio añadido es indicar los centros educativos en el área del domicilio del ciudadano, no será preciso facilitar otros datos como su fecha de nacimiento e incluso no será preciso el domicilio completo, siendo suficiente con conocer la calle o incluso el área en que tiene su residencia, lo que requiere que la comunicación de datos deba valorarse caso por caso.

Otra cuestión que se plantea es la relativa al uso de información calificada como datos abiertos, debe aquí tenerse en cuenta lo señalado en el primer punto del presente informe respecto de la necesidad de que los datos ofrecidos para su reutilización estén suficientemente agregados, de modo que no sea posible asociar los mismos a otros que obtengan los prestadores de servicios añadidos, así si los datos calificados como open data, aparentemente anónimos, son asociables a los datos de quien solicita un servicio, el prestador de servicios dispondría de un conjunto de datos del interesado sin que este haya prestado su consentimiento para un tratamiento de tal extensión.

Desde el punto de vista de la seguridad del sistema, habrá que analizar en cada caso las fórmulas de comunicación de los datos y si las mismas son conformes a las necesidades de seguridad del fichero público de que se trate. En todo caso, será preciso garantizar que la cesión de datos está limitada al

interesado que la ha consentido, y dentro de ella a los datos precisos conforme al principio de proporcionalidad. Debe atenderse especialmente al riesgo de que se produzcan descargas masivas de datos.

En segundo lugar, debe tenerse en cuenta que los servicios administrativos y los comerciales se encuentran sometidos a diferentes regímenes jurídicos. Los servicios administrativos se encuentran sujetos a la normativa administrativa y tienen en la mayor parte de los supuestos carácter obligado para la Administración, mientras que los servicios añadidos son servicios privados sujetos a la normativa mercantil y que pueden prestarse en régimen de libre concurrencia por las empresas. Ello determina que estén sometidos a diferentes normativas e incluso, dentro de la aplicación de la normativa de protección de datos, común a ambos, a la existencia de previsiones especiales para tratamientos de datos realizados por las Administraciones Públicas.

Así por ejemplo, en cuanto al servicio administrativo elegido en el proyecto, la emisión de un certificado del Padrón Municipal debe tenerse en cuenta que estará sujeto a todos los requisitos impuestos por la normativa que permite que se efectúe por medios electrónicos. Dispone así el artículo 29 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos lo siguiente:

"1. Las Administraciones Públicas podrán emitir válidamente por medios electrónicos los documentos administrativos a los que se refiere el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que incorporen una o varias firmas electrónicas conforme a lo establecido en la Sección 3.ª del Capítulo II de la presente Ley.

2. Los documentos administrativos incluirán referencia temporal, que se garantizará a través de medios electrónicos cuando la naturaleza del documento así lo requiera.

3. La Administración General del Estado, en su relación de prestadores de servicios de certificación electrónica, especificará aquellos que con carácter general estén admitidos para prestar servicios de sellado de tiempo."

Por su parte, el artículo 46 de la Ley 30/1992 a que se refiere dicho precepto dispone en su número 4 que *"Tienen la consideración de documento público administrativo los documentos válidamente emitidos por los órganos de las Administraciones Públicas."* Por su parte, el artículo 45.5 de la misma Ley dispone que *"Los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por ésta u otras Leyes."*

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que deroga la Ley 30/1992 y cuya entrada en vigor está prevista para el 2 de octubre del presente año, dispone en su artículo 26 respecto de la emisión de documentos por las Administraciones Públicas lo siguiente:

"1. Se entiende por documentos públicos administrativos los válidamente emitidos por los órganos de las Administraciones Públicas. Las Administraciones Públicas emitirán los documentos administrativos por escrito, a través de medios electrónicos, a menos que su naturaleza exija otra forma más adecuada de expresión y constancia.

2. Para ser considerados válidos, los documentos electrónicos administrativos deberán:

- *a) Contener información de cualquier naturaleza archivada en un soporte electrónico según un formato determinado susceptible de identificación y tratamiento diferenciado.*

- *b) Disponer de los datos de identificación que permitan su individualización, sin perjuicio de su posible incorporación a un expediente electrónico.*
- *c) Incorporar una referencia temporal del momento en que han sido emitidos.*
- *d) Incorporar los metadatos mínimos exigidos.*
- *e) Incorporar las firmas electrónicas que correspondan de acuerdo con lo previsto en la normativa aplicable.*

Se considerarán válidos los documentos electrónicos, que cumpliendo estos requisitos, sean trasladados a un tercero a través de medios electrónicos."

Asimismo, resultan de aplicación a las Administraciones Públicas Locales, por constituir normativa básica, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, por lo que las actuaciones a realizar por el Ayuntamiento consultante utilizando nuevas tecnologías exige dar cumplimiento a las especificaciones contenidas en dichas normas.

Por consiguiente, la Administración emisora del documento administrativo en cuestión deberá dar cumplimiento a todos los requisitos exigibles conforme a tal normativa, siendo responsable de los incumplimientos que de tales normas se produzcan.

Por su parte, las empresas que pretenden dar servicios añadidos, como cesionarias de los datos personales que con consentimiento del interesado se les faciliten, resultarán responsables de los datos que reciban quedando sujetas a todas las obligaciones y responsabilidades exigibles conforme a la normativa de protección de datos. Asimismo, en tanto tengan la condición de

empresas prestadoras de servicios de la sociedad de la información, tal y como se definen en el apartado c) del Anexo a la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, deberán dar cumplimiento a las previsiones de tal Ley, en particular, en materias de la competencia de esta Agencia, a lo previsto en el artículo 22.2, relativo al consentimiento para utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los usuarios (cookies u otro tipo de dispositivos), resultando responsables de la vulneración de lo previsto en dicha normativa, obligaciones éstas que, en conforme en principio no alcanzan a la Administración actuante.

Un tercer aspecto, se refiere al servicio de cloud computing**.** Debe así partirse de que la inclusión de datos personales en servicios de computación en nube solamente será conforme a lo establecido en la normativa de protección de datos si existe un contrato de prestación de servicios con el proveedor de servicios de cloud computing, en tanto los proveedores de servicios de computación en nube tendrán siempre la condición de encargados del tratamiento. Debe así tener en cuenta el responsable del tratamiento que su responsabilidad no se desplaza al proveedor del servicio aunque sea una gran compañía multinacional o incorpore una cláusula al respecto. En cuanto a la normativa de protección de datos aplicable será la del país en que esté establecido el responsable del tratamiento que contrata los servicios de computación en nube y no la del lugar en que se encuentren los proveedores de dichos servicios. Por consiguiente, el contrato de prestación de servicios con el proveedor de servicios de cloud computing deberá ajustarse a la normativa española.

Debe a este respecto tomarse en consideración lo señalado por esta Agencia en la guía publicada para facilitar el cumplimiento de la normativa de protección de datos a las entidades que contraten servicios de computación en nube. Dicha guía recuerda que las Administraciones Públicas, están sujetas,

además de a la Ley Orgánica 15/1999 y su Reglamento de desarrollo, a un marco legal específico al cual debe adecuarse la prestación de servicios basados en cloud computing, y que está constituido por la Ley de Contratos del Sector Público. (RD Legislativo 3/2011, de 14 de noviembre); la Ley 11/2007 de Acceso Electrónicos de los Ciudadanos a los Servicios Públicos; el RD 1671/2009 que desarrolla parcialmente esta ley; El Esquema Nacional de Seguridad y el Esquema Nacional de Interoperabilidad (Reales Decretos 3/2010 y 4/2010, de 8 de enero a los que ya se ha hecho referencia anteriormente).

La guía recuerda, asimismo, que la contratación por parte de las Administraciones Públicas de servicios cloud computing que impliquen el tratamiento de datos de carácter personal requiere la formalización de un contrato escrito en los términos previstos en el artículo 12 de la Ley Orgánica 15/1999 y en los artículos 20 a 22 de su reglamento de desarrollo. Dichos requisitos han sido específicamente recogidos en el ámbito de la contratación pública en la disposición adicional vigesimosexta del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público.

Por otra parte, en los servicios de cloud computing es frecuente que el encargado del tratamiento, esto es, el proveedor de los servicios, subcontrate servicios a terceros que también acceden a los datos personales. La guía de la Agencia señala, respecto de la subcontratación, que la disposición adicional vigésima sexta del Real Decreto Legislativo 3/2011, de 14 de noviembre, regula la subcontratación de servicios por parte del encargado del tratamiento, exigiendo lo siguientes requisitos:

"- Que dicho tratamiento se haya especificado en el contrato firmado por la administración contratante y el prestador de servicios de computación en la nube.

- Que el tratamiento de datos de carácter personal se ajuste a las instrucciones de la Administración que actúa como responsable del tratamiento.

- Que el prestador de servicios encargado del tratamiento y el tercero formalicen el contrato en los términos previstos en el artículo 12.2 de la LOPD."

En lo que se refiere a medidas de seguridad, aclara dicha guía que *"Los contratos de prestación de servicios de cloud computing deben especificar las medidas técnicas y organizativas que el prestador de servicios tiene previsto implantar para garantizar la seguridad de los datos. Asimismo, los especiales requisitos de disponibilidad, confidencialidad e integridad que puedan requerir ciertos servicios electrónicos prestados por las Administraciones Públicas (por ejemplo en el caso de las sedes electrónicas) deben reflejarse en el contrato mediante un acuerdo de nivel de servicio (SLA) en el que se especifiquen los indicadores de calidad de servicio que van a ser medidos y los valores mínimos aceptables de los mismos."*

Añade que "*En ciertos casos, la complejidad de los servicios contratados puede aconsejar la designación de un responsable del contrato en los términos previstos en el artículo 52 del RDL 3/2011, de 14 de noviembre, con el fin de asegurar la correcta realización de la prestación pactada. No obstante, la designación de dicha figura no modifica el régimen de obligaciones y responsabilidades al que está sujeto el responsable del tratamiento en materia de protección de datos de carácter personal*"

Asimismo la guía especifica las siguientes cuestiones:

"La prestación de servicios por encargados de tratamiento en cloud debería quedar claramente identificada en el documento de seguridad.

Asimismo, el acceso a la información debe reunir un nivel de medidas de seguridad equivalente al de los accesos en modo local, en la forma dispuesta por el Título VIII del RLOPD.

Además, la implantación de servicios de cloud computing incide de forma singular en algunos elementos del Esquema Nacional de Seguridad como los siguientes:

• ***Análisis y gestión de riesgos.*** *La migración de servicios y aplicaciones a entornos de cloud computing debe ser objeto de un análisis de riesgos que, en función de la sensibilidad de los datos y el nivel de amenazas, determine, en primer lugar, la conveniencia de esta solución y, en caso afirmativo, los controles y salvaguardas que deben implantarse para mitigar los riesgos hasta un nivel que pueda ser considerado aceptable.*

• ***Profesionalidad.*** *Conlleva la necesidad de que, en cualquier modalidad de prestación de servicios en la nube, la seguridad esté atendida, revisada y auditada por personal cualificado.*

• ***Protección de la información almacenada y en tránsito.*** *Debido a la especial sensibilidad de los datos tratados por las Administraciones Públicas, la aplicación de técnicas robustas de cifrado tanto a los datos en tránsito como a los datos almacenados constituye una medida necesaria para garantizar su confidencialidad. Asimismo, el contrato de prestación de servicios en la nube debe contemplar la realización de copias de respaldo de la información de forma que se garantice la plena disponibilidad e integridad de los datos almacenados.*

• ***Incidentes de seguridad y continuidad de la actividad.*** *La adopción de modelos de servicio basados en cloud computing debe contemplar una adecuada gestión de las incidencias de seguridad y mecanismos que*

garanticen la continuidad de las operaciones en caso de catástrofes o incidentes severos.

• ***Auditoría de la seguridad.*** *La contratación de servicios de cloud computing exige garantizar la realización de las auditorías de seguridad ordinarias y extraordinarias previstas en el artículo 34 del Esquema Nacional de Seguridad. Este artículo exige requisitos específicos sobre los criterios, métodos de trabajo y de conducta utilizados; los aspectos respecto de los que debe determinar la auditoría y los criterios metodológicos utilizados."*

En lo que se refiere a portabilidad e interoperabilidad la guía señala lo siguiente: *"La contratación de servicios de cloud computing por parte de las Administraciones Públicas debe garantizar la portabilidad de los datos entre prestadores de servicios y el ejercicio de los derechos de acceso por parte de los ciudadanos, mediante el uso de formatos estandarizados de datos que cumplan los requisitos establecidos en el Esquema Nacional de Interoperabilidad:*

• *Los documentos y servicios de administración electrónica que se pongan a disposición de los ciudadanos o de otras Administraciones Públicas deben encontrarse disponibles, como mínimo, mediante estándares abiertos. Asimismo, deben ser visualizables, accesibles y funcionalmente operables en condiciones que permitan satisfacer el principio de neutralidad tecnológica y eviten la discriminación a los ciudadanos por razón de su elección tecnológica.*

• *Deben adoptarse medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida.*

• *Conservación de los documentos electrónicos en el formato en el que hayan sido elaborados, enviados o recibidos, y preferentemente en un formato*

correspondiente a un estándar abierto que preserve a lo largo del tiempo la integridad del contenido de los documentos, de la firma electrónica y de los metadatos que lo acompañan."

Debe tenerse en cuenta también, que, como consecuencia del encargo del tratamiento o de las sucesivas subcontrataciones, puede originarse una transferencia internacional de datos, tal y como ésta viene definida en el artículo 5.1 s) del Reglamento de desarrollo de la Ley Orgánica 15/1999, transcrito anteriormente en el presente informe.

Dicha circunstancia es característica de la computación en nube, como se indica en el Dictamen 5/2012 sobre la computación en nube, emitido por el Grupo de Trabajo del artículo 29, según el cual "*la computación en nube se basa a menudo en la total falta de ubicación estable de los datos en la red del proveedor. Los datos pueden encontrarse en un centro de datos a las 2 horas y en el otro lado del mundo a las 16 horas. Por tanto el cliente rara vez se encuentra en posición de saber en cualquier momento en que lugar están situados, almacenados o transferidos los datos."*

De este modo la transmisión de datos a entidades situadas fuera del Espacio Económico Europeo, como anteriormente se ha indicado ya, constituirá una transferencia internacional de datos que deberá respetar el régimen establecido en los artículos 33 y 34 de la Ley Orgánica 15/1999 y en el Título VI de su Reglamento de desarrollo, a que anteriormente se ha hecho referencia. Ello determina que el consultante deba conocer la cadena de subcontrataciones a fin de estar informado donde pueden localizarse los datos y si el país tiene un régimen de garantías adecuado, debiendo solicitar la correspondiente autorización de la Agencia en caso contrario. Señala en este sentido el Dictamen 5/2012 que la transparencia en la nube supone que es necesario que el cliente tenga conocimiento de todos los subcontratistas que contribuyan a la prestación de los respectivos servicios en nube, así como de la

localización de todos los centros donde puedan tratarse los datos personales. Sólo entonces podrá evaluar si los datos personales pueden ser transferidos a un llamado tercer país fuera del Espacio Económico Europeo (EEE) que no garantice un nivel adecuado de protección en el sentido de la Directiva 95/46/CE.

Debe tenerse en cuenta, en lo que respecta a las transferencias de datos a Estados Unidos, que la sentencia de 6 de octubre de 2015 del Tribunal de Justicia de la Unión Europea declaró inválida la decisión 2000/520/CE que declaraba el nivel adecuado de protección de las garantías para las transferencias internacionales de datos a Estados Unidos, ofrecidas por el Acuerdo de Puerto Seguro, si bien tales transferencias, hasta tanto se firme un nuevo acuerdo, podrán ampararse en otras bases legales como las Cláusulas Contractuales Tipo adoptadas por las Decisiones de la Comisión Europea 2001/497/CE, 2004/915/CE y 2010/87/UE .

No obstante, las dificultades que plantean a los responsables del fichero o tratamiento la necesidad de recabar en cada caso la autorización del director de esta Agencia para la transferencia internacional de datos podrían ser obviadas, como se señalaba en informe de esta Agencia, en el supuesto de que por el prestador del servicio de cloud computing se adoptasen unas cláusulas estandarizadas que, conteniendo las garantías adecuadas de protección de los derechos de los afectados, y en particular de su derecho fundamental a la protección de datos, fuesen aprobadas por esta Agencia. Existiría así una autorización automática de cualquier transferencia internacional realizada al amparo de tales cláusulas en tanto no se produjera ninguna alteración de las mismas, de modo que el cliente (esto es, el responsable del fichero) únicamente tendría que notificar la modificación del fichero cuyos datos fueran objeto de transferencia como consecuencia de la contratación del servicio de computación en nube.