N/REF: 322908/2016

Se solicita de la Agencia Española de Protección de Datos una evaluación y recomendación de acciones a tomar durante la implementación del proyecto denominado PRISMA CLOUD (Privacy and Security maintaining services in the cloud) incluido en el ámbito del programa Horizonte 2020 de la Unión Europea.

Según señala la documentación aportada, el proyecto tiene entre sus objetivos desarrollar nuevas técnicas criptográficas para proteger la seguridad de los datos en la nube durante todo su ciclo de vida (en reposo, en movimiento o en uso) y la privacidad de los usuarios.

En el marco del proyecto se van a realizar encuestas, talleres y demostraciones en diferentes escenarios piloto en las áreas de Smartcities, E-Government y E-Health. Según señala la documentación aportada en las demostraciones no se pretende trabajar con datos reales, si bien potencialmente pueden recogerse o tratarse datos personales de los usuarios que participan en las pruebas o de otras partes interesadas que participen en los ensayos y estudios de usabilidad.

En el proyecto participan diversas entidades españolas, de países miembros de la Unión Europea y de Israel.

I

La primera cuestión que resulta del proyecto sujeto a informe es la relativa a la aplicación en el tiempo de la normativa de protección de datos, teniendo en cuenta la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Las previsiones de dicha norma resultarán de aplicación a partir del 25 de mayo de 2018, conforme a lo previsto en su artículo 99.2.

Por consiguiente, se aplicarán hasta dicha fecha las normas que hasta ahora venía rigiendo la materia, esto es 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, y la normativa que en cada país la desarrolla, normativa que en España viene constituida fundamentalmente por La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter Personal y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre y con posterioridad al 25 de mayo de 2018 el citado Reglamento General de Protección de datos, lo que debe tenerse en cuenta si la ejecución del proyecto se extiende hasta un momento posterior a la aludida fecha.

En segundo lugar, debe examinarse la aplicabilidad de la normativa de protección de datos a los tratamientos de datos que puedan llevarse a cabo durante la ejecución del proyecto objeto de consulta, para ello debe examinarse el concepto de dato personal, definido en el artículo 3.a) de la Ley Orgánica 15/1999 como "*cualquier información concerniente a personas físicas identificadas o identificables."* El artículo 5.1 de su Reglamento de desarrollo precisa 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."*

Dicha definición procede del artículo 2 de 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, según el cual se entenderán por datos personales *"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».*

Cabe así recordar lo señalado por 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, en su Dictamen 4/2007 sobre el concepto de datos personales, en el que tras poner de manifiesto que la Directiva maneja un concepto lato de datos personales, analiza los elementos de dicha definición, indicando respecto a la expresión "toda información" lo siguiente:

"Desde el punto de vista de la naturaleza de la información, el concepto de datos personales incluye todo tipo de afirmaciones sobre una persona. Por consiguiente, abarca información «objetiva» como, por ejemplo, la presencia de determinada sustancia en su sangre, pero también informaciones, opiniones o evaluaciones «subjetivas». Esta última clase de afirmaciones constituye una parte considerable del caudal de datos personales tratados en sectores como el de la banca, para evaluar la fiabilidad de los prestatarios («Fulano es un

prestatario fiable»), el asegurador («no se espera que Fulano muera pronto») o el laboral («Fulano es un buen trabajador y merece un ascenso»).

Para que esas informaciones se consideren «datos personales», no es necesario que sean verídicas o estén probadas. De hecho, las normas de protección de datos prevén la posibilidad de que la información sea incorrecta y confieren al interesado el derecho de acceder a esa información y de refutarla a través de los medios apropiados.

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.).”

Como continuación de dicho análisis el Grupo de trabajo examina el término “sobre” indicando que “*ya se ocupó anteriormente de la cuestión de cuándo puede considerarse que una información versa «sobre» una persona. En el marco de sus debates sobre los problemas de protección de datos planteados por las etiquetas RFID, el Grupo de trabajo señaló que un «dato se refiere a una persona si hace referencia a su identidad, sus características o su comportamiento o si esa información se utiliza para determinar o influir en la manera en que se la trata o se la evalúa».*

A este respecto, cabe recordar que tanto la voz como la imagen de las personas identificadas o identificables tienen la consideración de datos personales. En este sentido, el Dictamen 02/2012 del Grupo de Trabajo del artículo 29 sobre reconocimiento facial en los servicios en línea y Móviles al hacer referencia a las imágenes digitales como datos personales señala que ***“****Si en una imagen digital se distingue tan claramente el rostro de una persona que es posible identificarla, dicha imagen se consideraría un dato personal. Ello dependerá de una serie de parámetros, como la calidad de la imagen o el encuadre concreto. En la mayoría de los casos no se considerarían datos personales las imágenes de escenas en las que se ve a personas en la distancia, o en las que los rostros están difuminados.”*

Además, cabe recordar que el Reglamento (UE) 2016/679, esto es, el Reglamento General de Protección de Datos, hace expresa mención a otros tipos de datos personales en la definición que de los mismos efectúa en su

artículo 4.1, entendiendo por tales *"toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.*

Dicha definición tiene en cuenta la aparición de nuevos datos identificativos de las personas, tal y como expresa su considerando 30 según el cual "*Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas."*

De este modo tendrán la condición de datos personales todas las informaciones asociadas a las personas físicas que participen en el proyecto objeto de consulta, incluidas su voz y su imagen si las mismas son captadas en la realización de alguna de las actividades.

Debe, asimismo, hacerse referencia al concepto de tratamiento de datos personales, toda vez que de lo expuesto en el proyecto se desprende la realización de diversos posibles tratamientos. A este respecto, 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 alguna o varias de estas operaciones respecto de datos personales constituirá un tratamiento de datos personales. Debe así tenerse en cuenta que la recogida de datos no constituye el único tratamiento posible, sino que otras operaciones (por ejemplo, conservación, elaboración, modificación o comunicaciones de datos) constituyen también tratamientos de datos personales y son igualmente determinantes, de la aplicabilidad de la normativa de protección de datos.

II

Teniendo en cuenta que en el proyecto participan, junto a las entidades españolas, entidades de otros Estados miembros de la Unión Europea, debe considerarse cuál es la normativa aplicable.

El artículo 4 de 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 dispone al respecto:

1 *Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:*

a *el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable"*

Para determinar la legislación aplicable resulta necesario hacer referencia a las figuras de responsable y encargado del tratamiento. El artículo 2 de la Directiva 95/46 define en su letra d) al responsable del tratamiento como *"la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales;* (…)" Debe así diferenciarse el responsable del fichero o tratamiento del responsable del proyecto o de una fase del mismo ya que a dicha condición de responsable del fichero o tratamiento se anudan determinadas consecuencias jurídicas distintas a las propias de quien está a cargo de un determinado trabajo.

Cabe así señalar, con carácter general, que la condición de responsable del fichero es consecuencia del hecho de que una persona o entidad, debidamente legitimada, haya decidido tratar datos personales para sus propios fines, correspondiéndole por ello asumir las obligaciones impuestas por la normativa de protección de datos y las responsabilidades que de su incumplimiento pudieran derivarse. En el derecho español la Ley Orgánica 15/1999, define al responsable del fichero o tratamiento como la *"persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".*

Por su parte, el encargado del tratamiento viene definido en el artículo 2.e) de la Directiva como *"la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento."*

Cabe así recordar que esta figura obedece 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 por parte del responsable a quien le presta tal servicio, sino que el tratamiento de los datos se realiza por el encargado en nombre y por cuenta del responsable como si fuera este mismo quien lo lleva a cabo. El artículo 3 g) de la Ley Orgánica 15/1999, define así al encargado como "*la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento*".

Debe tenerse en cuenta que, para que pueda hablarse de encargado del tratamiento la Directiva 95/46/CE, viene a exigir los siguientes requisitos en su artículo 17:

"*1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.*

Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

2. Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.

3. *La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:*

- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;

- que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

4. A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente."

De este modo, si las entidades participantes en el proyecto establecidas en un Estado miembro actúan en calidad de responsables deberán ajustar los tratamientos de datos que efectúen a lo previsto en la normativa de protección de datos que les resulte de aplicación, de conformidad con lo establecido en el artículo 4 de la Directiva 95/46/CE, esto es, los tratamientos de datos personales en el marco de las actividades de cada establecimiento deberán adecuarse a la legislación nacional en que cada establecimiento se encuentre.

En el caso de que las entidades participantes en el proyecto actúen como encargados del tratamiento, les resultará de aplicación la normativa de protección de datos que corresponda al responsable por cuya cuenta actúan, excepto en lo que respecta a la adopción de medidas de seguridad, en que se aplicará la normativa del Estado miembro en que tenga su establecimiento el encargado del tratamiento.

En el presente supuesto parece desprenderse de la documentación aportada en la consulta que respecto de algunas de las actividades a llevar a cabo en el proyecto, una de las entidades españolas actúa en calidad de encargado del tratamiento de otra entidad participante en el proyecto establecida en otro país de la Unión Europea. Se aporta un modelo de consentimiento en el que se indica que el responsable será la entidad extranjera y que se aplicará al tratamiento de los datos la normativa del país del responsable, la Directiva 95/46/CE y el Reglamento General de Protección de datos.

En este sentido debe recordarse que para que tal relación entre el encargado de tratamiento y el responsable exista y sea válida, la Directiva 95/46/CE, normativa vigente en este momento, exige la existencia de un **"***contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento"* que deberá plasmarse por escrito u otra forma equivalente y que deberá contener al menos las especificaciones exigidas en el número 3 del artículo 17, sin perjuicio de que la normativa del país del responsable pueda contener mayores exigencias. La inexistencia de dicho acto jurídico, dará lugar a que el encargado del tratamiento devenga responsable del mismo, debiendo, en tal caso, responder conforme a la normativa de protección de datos española.

En todo caso, el encargado del tratamiento cuyo establecimiento se encuentra en España debe adoptar las medidas de seguridad exigibles conforme a la normativa española, conforme a lo dispuesto en el artículo 7.3 de la Directiva 95/46/CE.

En este sentido cabe recordar que el artículo 9 de la Ley Orgánica 15/1999 dispone que *"El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y*

los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural."

El número 2 de dicho precepto prohíbe el registro de datos de carácter personal en ficheros "*que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas."*

Debe, además, recordarse que, como ha señalado reiteradamente la Audiencia Nacional en sus sentencias (por todas ellas SAN de 6-10-2011), la seguridad constituye una obligación de resultado consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros.

El Reglamento de desarrollo de la Ley Orgánica 15/1999, constituye en la actualidad la normativa vigente en materia de medidas de seguridad aplicables a los tratamientos de datos de carácter personal. El artículo 80 de esta norma clasifica las medidas de seguridad aplicables a los ficheros o tratamientos de datos en tres niveles, debiendo adoptarse, en cada caso, el nivel correspondiente en función de la naturaleza de los datos a tratar. Debe tenerse presente, además, que dichas medidas tienen un carácter acumulativo, de forma que las establecidas para cada nivel exigen incorporar las previstas para los niveles inferiores.

No obstante, debe hacerse una referencia a la regulación que en materia de medidas de seguridad será aplicable a partir del 25 de mayo de 2018, en tanto que el Reglamento (UE) 2016/679 (Reglamento general de protección de datos) adopta un enfoque diferente al establecido en la Ley Orgánica 15/1999 y su normativa de desarrollo en lo que respecta a las medidas de seguridad que el responsable de un fichero debe implementar.

Señala el considerando 83 de dicha norma que *" A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales."*

Y en su artículo 32, números 1 y 2, dispone lo siguiente respecto de la seguridad del tratamiento:

"1.Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a*) la seudonimización y el cifrado de datos personales;*

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."

Asimismo, debe tenerse en cuenta que, una vez resulte de aplicación el Reglamento (UE) 2016/679, incumbirá a todos los responsables la obligación de notificar, en su caso, las violaciones de seguridad de los datos a la autoridad de control (en el caso de responsables españoles a la Agencia Española de Protección de Datos) y la obligación del encargado de tratamiento de notificar al responsable sin dilación aquéllas de que tenga conocimiento. Dispone el artículo 33 de dicho Reglamento que:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente

de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

La notificación contemplada en el apartado 1 deberá, como mínimo:

a *describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;*

b *comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;*

c *describir las posibles consecuencias de la violación de la seguridad de los datos personales;*

d *describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.*

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación

permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."

III

En lo que respecta a la aplicación de la normativa de protección de datos española el artículo 3.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999, dispone que "*Se regirá por el presente reglamento todo tratamiento de datos de carácter personal: a) Cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español."*

De este modo, los tratamientos de datos realizados por responsables cuyo establecimiento se encuentre en territorio español quedarán sujetos a lo dispuesto en la Ley Orgánica 15/1999, salvo que como se ha visto anteriormente actúen en calidad de encargados del tratamiento de un responsable situado en otro Estado de la Unión Europea. Este será el caso de las demás entidades españolas participantes en el proyecto si actúan en calidad de responsables, pero sería igualmente el caso de cualquier otra entidad participante si tuviera un establecimiento en España y efectuase un tratamiento de datos en el marco de las actividades del mismo. También quedarán sometidas a la normativa española de protección de datos las entidades que actúen como encargadas de tratamiento de responsables sujetos a la normativa española, excepto en la aplicación de las medidas de seguridad que serán las del país en que tenga su establecimiento el encargado.

Por consiguiente, las entidades españolas que tengan la condición de responsables del tratamiento o que, conforme a lo señalado, queden sujetas a la normativa de protección de datos española, deberán dar cumplimiento a las previsiones contenidas en la Ley Orgánica 15/1999, entre las cuales deben destacarse las siguientes:

-Deberá notificarse la creación del fichero a efectos de su inscripción en el Registro General de Protección de Datos de esta Agencia.

-Será preciso implantar en el fichero creado las debidas medidas de seguridad establecidas en el Reglamento de desarrollo de la Ley Orgánica 15/1999, debiendo igualmente tenerse en cuenta lo señalado respecto a las medidas de seguridad a adoptar y obligaciones de notificar las violaciones de seguridad de los datos que impone el Reglamento General de Protección de Datos una vez resulte aplicable.

- Requisito capital para que un tratamiento de datos personales sea conforme a lo establecido en la normativa de protección de datos es que el mismo se encuentre legitimado en alguna de las causas recogidas en el artículo 6 de la Ley Orgánica 15/1999 cuyo número primero exige el consentimiento inequívoco del afectado salvo que la Ley disponga otra cosa.

De este modo, el responsable deberá recabar, de las personas físicas que participen en las diversas actividades previstas en el proyecto, su consentimiento para el tratamiento de sus datos personales, consentimiento que deberá reunir las características de "libre, inequívoco, específico e informado" conforme a lo previsto en el artículo 3.h) de la Ley Orgánica 15/1999.

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.

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.

IV

Si alguna de las entidades sujetas a la normativa de protección de datos española efectuasen una comunicación de los datos personales objeto de tratamiento en el proyecto a terceros, incluidas las demás entidades que participan en el mismo, o procediesen a su difusión por cualquier

procedimiento, dicha comunicación o difusión constituirá una cesión de datos personales definida en el artículo 3 i) de la Ley Orgánica 15/1999 como "*Toda revelación de datos realizada a una persona distinta del interesado".*

Tal cesión debe sujetarse al régimen general de comunicación de datos de carácter personal establecido en el artículo 11 de la Ley Orgánica 15/1999, donde se establece que la misma solo puede verificarse para el cumplimiento de fines directamente relacionados con las funciones legitimas del cedente y cesionario y exige, para que pueda tener lugar, el consentimiento del interesado (artículo 11.1), otorgado con carácter previo a la cesión y suficientemente informado de la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar (artículo 11.3), y que debe recabar el cedente como responsable del fichero que contiene los datos que se pretenden ceder.

No obstante, cabe recordar la posibilidad de que las demás entidades participantes en el proyecto puedan actuar en condición de encargados del tratamiento del responsable. El artículo 12 de la Ley Orgánica 15/1999 regula la figura del encargado del tratamiento, disponiendo que *"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*."

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".*

Esta Agencia Española de Protección de Datos ha venido indicando que el deber de devolución al que se refiere el artículo 12.3 de la aludida Ley Orgánica podrá verificarse mediante la entrega directa de los datos al propio responsable del tratamiento o mediante la realización de dicha entrega al encargado del tratamiento que este designase, toda vez que en este segundo caso el encargado actuaría como mero mandatario del responsable, siendo precisamente éste el que establece a quién han de entregarse los datos en su nombre y por su cuenta. Y así se recoge en el artículo 20.3 del Reglamento de desarrollo de dicha Ley al disponer "*no obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo."*

Por su parte, el artículo 22 del aludido Reglamento dispone respecto de la conservación de los datos lo siguiente:

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

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento."

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, con la excepción antes señalada respecto de la adopción de medidas de seguridad cuando el encargado tenga su establecimiento en otro

Estado miembro de la Unión Europea. Deben tenerse en cuenta igualmente las nuevas exigencias que impone en materia de medidas de seguridad y notificación de violaciones de seguridad el Reglamento General de Protección de Datos.

V

Debe además recordarse que todo tratamiento de datos debe ser respetuoso de los principios relativos a la calidad de los datos contenidos en la Directiva 95/46 CE. En este sentido, la Ley Orgánica 15/1999, recoge igualmente dichos principios, debiendo destacarse en particular el denominado principio de finalidad, recogido en el artículo 4.2 de dicha Ley y conforme al cual "*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 aclararse aquí que la Audiencia Nacional partiendo de una interpretación sistemática de este precepto viene considerando la expresión "finalidades incompatibles" como sinónimo de "finalidades distintas".

De este modo no resultaría posible la utilización de los datos personales para una finalidad distinta a aquélla para la que se solicitó el consentimiento de los interesados, sin que nuevamente se recabe éste de manera informada o sin que dicho nuevo tratamiento encuentre su legitimación en alguno de los supuestos contenidos en el artículo 6 de la Ley Orgánica 15/1999.

Igualmente, dentro de tales principios, debe hacerse referencia al relativo a la conservación de los datos, disponiendo el número 5 del artículo 4 de la Ley Orgánica 15/1999 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.*

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

En consecuencia, los datos personales recogidos no podrán mantenerse indefinidamente en los ficheros de los participantes en el proyecto, debiendo cancelarse una vez que dichos datos dejen de ser necesarios para la finalidad para la cual fueron obtenidos. Como norma general los proyectos vienen fijar un plazo de cancelación de un año o dos tras su conclusión, entendiendo que en tal momento los datos personales no resultan ya precisos. En la documentación aportada no se establece un plazo con carácter general pero se señala que los datos serán eliminados o anonimizados tan pronto como sea posible.

Cabe recordar que el Reglamento Europeo de Protección de Datos, además de regular en su artículo 5.1.e) el principio de limitación del plazo de conservación, refuerza el mismo añadiendo un principio de responsabilidad proactiva en el número 2 del mismo artículo 5, de modo que el responsable debe no solamente responder del cumplimiento de tal principio (y del de los demás principios regulados en dicho precepto) sino ser capaz de demostrar su cumplimiento. En este sentido, impone ya desde el momento en que se recaba información del interesado la obligación de informarle del plazo durante el cual se conservarán los datos personales o, cuando no sea posible, de los criterios para determinar tal plazo.

VI

Por último, debe tenerse en cuenta que la transmisión de datos personales a entidades situadas fuera del Espacio Económico Europeo constituye una transferencia internacional de datos. Si dicha transmisión fuese realizada por un responsable establecido en España deberá respetar el régimen regulado en los artículos 33 y 34 de la Ley Orgánica 15/1999 y en el Título 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 y Canadá respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos.

En tanto que la Comisión de la Unión Europea ha considerado que existe un nivel de protección adecuado en Israel, no sería precisa la autorización del Director de la Agencia Española de protección de Datos. No obstante, la transferencia internacional de datos deberá declararse en todo caso en el Registro General de Protección de Datos tal y como dispone el artículo 66.3 del Reglamento de desarrollo de la Ley Orgánica 15/1999, según el cual "*En todo caso, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos, conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.*"