N/REF: 176137/2016

Se solicita de la Agencia Española de Protección de Datos una evaluación y recomendación de acciones a tomar durante la implementación del proyecto denominado NOBEL GRID (NEW COST EFFICIENT BUSINESS MODELS FOR FLEXIBLE SMART GRIDS) incluido en el ámbito del programa Horizonte 2020 de la Unión Europea.

Según señala la documentación aportada, el proyecto tiene como objetivo desarrollar, desplegar y evaluar herramientas avanzadas y servicios TIC para los operadores de los sistemas de distribución y cooperativas eléctricas, permitiendo la participación activa de los consumidores y la flexibilidad del mercado, con nuevos modelos de negocio que faciliten la integración de la producción de energía renovable distribuida.

En el marco del proyecto se van a realizar, entre las actividades que comportan el tratamiento de datos de carácter personal, talleres, entrevistas, encuestas y demostraciones en varios sitios piloto, uno de ellos en una cooperativa eléctrica socia del proyecto situada en una población española. Entre las herramientas a utilizar en la demostración se encuentra una aplicación que, según se indica, permitirá a los consumidores domésticos e industriales visualizar, controlar y administrar su consumo y producción de energía en tiempo real, de forma que tengan una idea de lo que está sucediendo en su casa o en sus instalaciones con una visión del panel principal de la aplicación. Dicha herramienta estará disponible en forma de una aplicación web y móvil, recopilando información de energía de un medidor de electricidad instalado en la vivienda o las instalaciones, desde donde se enviará la información a un servidor central en las instalaciones del proveedor de servicios de la aplicación para su análisis y almacenamiento.

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

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 hacerse una referencia al ámbito de aplicación de la normativa de protección de datos. Debe así 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."*

En consecuencia las personas jurídicas no gozan de las garantías establecidas por la Ley Orgánica 15/1999. Así se establece expresamente en el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre, que en su artículo 2.2 dispone que *"Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas"*

El aludido reglamento, dispone igualmente en su artículo 2.3, en relación con los empresarios individuales que "*Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal."* Debe aquí hacerse referencia a la interpretación que esta Agencia ha realizado en sus informes respecto al alcance de este precepto, en los que se concluye lo siguiente:

> "Cabrá considerar que la legislación de protección de datos no es aplicable en los supuestos en los que los datos del comerciante

sometidos a tratamiento hacen referencia únicamente al mismo en su condición de comerciante, industrial o naviero; es decir, a su actividad empresarial.

Al propio tiempo, el uso de los datos deberá quedar limitado a las actividades empresariales; es decir, el sujeto respecto del que pretende llevarse a cabo el tratamiento es la empresa constituida por el comerciante industrial o naviero y no el empresario mismo que la hubiese constituido. Si la utilización de dichos datos se produjera en relación con un ámbito distinto quedaría plenamente sometida a las disposiciones de la Ley Orgánica."

Ahora bien, no cabe aplicar la exclusión contenida en el aludido artículo 2.3 a los profesionales autónomos. Como esta Agencia ha venido manifestando reiteradamente, existe una diferencia entre aquéllos y el empresario individual, de forma que los profesionales autónomos sólo quedarían excluidos de la aplicación de la Ley Orgánica 15/1999 en caso de que los mismos organicen su actividad en forma de empresa.

En este sentido se pronunciaba ya la Resolución de 27 de febrero de 2001, en el que se señalaba que a los profesionales les sería aplicable la Ley Orgánica 15/1999 "*cuando no tuvieran organizada su actividad profesional bajo la forma de empresa, no ostentando en consecuencia la condición de comerciante (es el caso de los profesionales liberales cuyas actividades están expresamente excluidas del ámbito de aplicación de la Ley Básica 3/1993 por su artículo 6).*"

Es éste también el criterio de la Audiencia Nacional que en sentencia de 21 de noviembre de 2002 considera aplicable la normativa de protección de datos vigente en el momento a profesionales liberales indicando que "aquellos datos se refieren a profesionales que no ejercen su actividad bajo forma de empresa, no ostentando en consecuencia la condición de comerciantes a la que se refieren los artículos primero y siguientes del Código de Comercio."

Por consiguiente, la protección conferida por la Ley Orgánica 15/1999 no comprende a las personas jurídicas, si bien sus disposiciones resultarán aplicables a los datos de las personas físicas que participen en las actividades previstas en el proyecto, aunque éstas actúen en nombre o representación de personas jurídicas. Dicha protección tampoco se extiende a los empresarios individuales cuando los tratamientos se refieran a ellos en su condición de comerciante, industrial o naviero, pero sí se extiende a los restantes supuestos. Sin embargo, debe tenerse en cuenta, que la exclusión contenida en el

Reglamento de desarrollo de la Ley Orgánica 15/1999, referida a los empresarios individuales, dejará de ser efectiva el 25 de mayo de 2018, fecha en que como se ha señalado, será aplicable el Reglamento (UE) 2016/679 (Reglamento general de protección de datos), norma que, como se ha señalado, sustituirá la vigente normativa nacional de protección de datos y que no exceptúa de su protección a los empresarios individuales.

En tercer lugar para determinar la aplicabilidad de la normativa de protección de datos debe, igualmente, examinarse el concepto de dato personal. Tal y como anteriormente se ha señalado, el artículo 3.a) de la Ley Orgánica 15/1999 define éstos 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."*

Cabe aquí 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».*

En este sentido, debe tenerse en cuenta que tanto la voz como la imagen de las personas identificadas o identificables tienen la consideración de datos personales. Así, 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, en el presente supuesto, tendrán la condición de datos de carácter personal cualquier clase de información, en los términos vistos, asociada a las personas físicas que en algún modo participan en las actividades previstas en el proyecto, así los datos que se recaban en los formularios que firman los participantes en entrevistas, encuestas, talleres, etc, pero también otros datos como la voz y la imagen si estos fueran captados en alguna de las actividades, los datos recogidos de los dispositivos de medición inteligentes, las direcciones de correo electrónico que pudieran recabarse, datos contenidos en el dispositivo móvil que sea preciso utilizar para el funcionamiento de la aplicación, etc. El tratamiento de cualquier clase de datos personal quedará sujeto a lo establecido en la normativa de protección de datos.

Debe, en este sentido 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, esto es, de cualquier información asociada a una persona física identificada o identificable, dará lugar a 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 y son igualmente determinantes, de la aplicabilidad de la normativa de protección de datos.

La consulta señala que respecto de la demostración los datos recabados serán anónimos, eliminando la información de identificación personal como nombre, apellidos, dirección, etc., de modo que no puedan ser identificados los participantes en la demostración miembros de la cooperativa española en la que aquélla se lleva a cabo.

Cabe así recordar que no resulta aplicable la normativa de protección de datos cuando no sea posible identificar a las personas, por haberse sometido sus datos a 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."*

Conforme al artículo 5.1.o del Reglamento de desarrollo de la Ley Orgánica 15/1999 es identificable *“toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.”*

Dicha definición tiene su origen en lo dispuesto en el artículo 2 de la aludida Directiva 95/46/CE, conforme al cual son 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».* Asimismo, tiene en cuenta el considerando 26 de dicha Directiva 95/46/CE en el que se señala 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”.*

Por parte de esta Agencia se ha venido señalando que para que un procedimiento de disociación pueda ser considerado suficiente a los efectos de la Ley Orgánica 15/1999, es necesario que de la aplicación de dicho procedimiento resulte imposible asociar el dato o datos de que se disponga a un sujeto determinado. Para ello será preciso que no exista la posibilidad, incluso remota, de que, mediante la utilización, con carácter previo, coetáneo o posterior de cualquier medio, la información concerniente a los afectados por el tratamiento de datos, que obre en poder del consultante, pueda revelar su identidad.

En esta materia resulta de especial interés lo señalado por el Grupo de Trabajo del artículo 29 en sus dictámentes. Así ya en su Dictamen 6/2013 indicaba que “*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.”*

En particular en el Dictamen 5/2014, sobre técnicas de anonimización, el citado Grupo de Trabajo señalaba que “*A la luz de la Directiva 95/46/CE y de otros instrumentos jurídicos pertinentes de la UE, la anonimización es el resultado de un tratamiento de los datos personales realizado para evitar de forma irreversible su identificación.”*

Se recordaba en dicho Dictamen 5/2014 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."

En dicho Dictamen 5/2014 se ponía igualmente de manifiesto 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."*

Por consiguiente, no cabe considerar que en el proyecto se tratan datos anónimos, en primer lugar, porque no lo son en el momento de su recogida, operación que por sí misma constituye un tratamiento de datos lo que ya determina la aplicación de la normativa de protección de datos. Por otra parte, de los distintos tratamientos de datos a llevar a cabo en el proyecto no se desprende que se proceda a una anonimización, ya que este requeriría que en ningún caso pudieran asociarse los diversos datos tratados a una persona física determinada, lo que resulta imposible teniendo en cuenta las actividades a llevar a cabo (entrevistas, talleres, etc. en los que incluso se prevé la

grabación de las personas). En lo que respecta a la señalada anonimización de los datos a utilizar durante la demostración cabe pensar en diversos elementos que permiten o pueden permitir la identificación de las personas físicas (por ejemplo, el correo electrónico que contenga el nombre del usuario o el acceso a datos personales contenidos en el dispositivo móvil a los que se precise acceder para el funcionamiento de la aplicación) por lo que no cabe hablar de anonimización. No obstante, debe valorarse positivamente la minimización del tratamiento de datos efectuado, como el que la localización se limite a una población sin especificar la ubicación exacta de las instalaciones del consumidor.

II

Teniendo en cuenta que en el proyecto participan entidades españolas y 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, números 3 y 4:

"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 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 la información aportada en la consulta no puede determinarse el carácter, desde el punto de vista de protección de datos, con que actúan los distintas entidades participantes en el proyecto, debe así tenerse en cuenta que 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. Este será el caso de la entidad española participante en el proyecto si actúa en calidad de responsable, 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. No obstante, si alguna entidad española actuase como encargado del tratamiento de un responsable al que deba aplicarse la normativa de protección de datos de otro país de la Unión Europea, seguirá la ley nacional del responsable, salvo en lo que respecta a las medidas de seguridad que serán las establecidas en la normativa española.

III

Las entidades españolas que tengan la condición de responsables del tratamiento deberán dar cumplimiento a las previsiones contenidas en la Ley Orgánica 15/1999, entre las cuales deben destacarse las siguientes:

En primer lugar, deberá notificarse la creación del fichero a efectos de su inscripción en el Registro General de Protección de Datos de esta Agencia.

En segundo lugar debe recordarse que el 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".*

Por consiguiente, el modelo de consentimiento aportado debe adecuarse a dichos requerimientos, identificando al responsable del tratamiento (que cómo se ha indicado no es el investigador, sin perjuicio de que se le señale como la persona ante la que puede ejercitar sus derechos) y se indique al particular la posibilidad de ejercer los derechos a que se refiere la letra d) de dicho precepto. Asimismo debe indicarse quienes son los posibles destinatarios de la información (en el presente supuesto, a título de ejemplo, otros socios del

proyecto en caso de que se les comunicasen datos personales) recabando el consentimiento de los interesados para tal comunicación de datos, igualmente, debe recabarse el consentimiento del interesado cuando se pretenda llevar a cabo la difusión por cualquier procedimiento de alguna de las actividades o de los datos obtenidos con motivo de éstas.

Corresponde al responsable del fichero acreditar que ha dado cumplimiento a dicha obligación de información, si bien tras la anulación de lo previsto en el artículo 18 del Reglamento de desarrollo de la Ley Orgánica 15/1999 por Sentencia de 15 de julio de 2010 del Tribunal Supremo, debe entenderse que rige la libertad de forma para acreditar el cumplimiento de la misma, de modo que el responsable podrá demostrar por cualquier medio de prueba admisible en derecho el cumplimiento del deber de informar exigido por el artículo 5 de la Ley Orgánica 15/1999.

Especial mención merece el deber de información en el caso de la aplicación a que la consulta se refiere, puesto que debe darse tal información antes de la instalación de la misma. En este sentido, el usuario de la aplicación tiene derecho a saber qué tipo de datos personales están siendo tratados y con qué finalidad se van a usar.

Siguiendo lo señalado por el Grupo de Trabajo del artículo 29 en su informe 02/2013 sobre las aplicaciones de los dispositivos inteligentes cabe recordar que el desarrollador de la aplicación es un responsable del fichero o tratamiento, en tanto que decide la medida en que la aplicación accederá y procesará las distintas categorías de datos personales en el dispositivo y o a través de recursos informáticos remotos, de modo que, de conformidad con la definición legal de responsable antes vista, determina los fines y los medios del tratamiento de datos personales en los dispositivos inteligentes. Por consiguiente le incumben todas las obligaciones exigibles al responsable del fichero o tratamiento. La categoría de desarrollador de la aplicación incluye tanto a las personas que crean una aplicación y la distribuyen como a las entidades públicas o privadas que subcontratan el desarrollo de la aplicación. En el presente supuesto parece desprenderse de la documentación aportada en la consulta que la aplicación se desarrolla como una parte del proyecto, de modo que tendría tal condición de desarrollador y en consecuencia de responsable, el miembro o miembros del proyecto que haga uso de la misma, sin perjuicio de quien resulte responsable si, fuera del marco del proyecto, se continúa utilizando dicha aplicación.

Señala dicho dictamen 02/2013 que el responsable del tratamiento debe informar a los usuarios potenciales como mínimo de la identidad y datos de contacto del responsable, de las categorías exactas de datos personales que el desarrollador de aplicaciones recogerá y tratará, de los objetivos precisos y si los datos se comunicasen a terceros la forma en que los usuarios pueden ejercer sus derechos (retirar el consentimiento y eliminar datos).

Ser informado de qué datos se están tratando es especialmente importante habida cuenta del amplio acceso que las aplicaciones suelen tener a sensores y estructuras del dispositivo, donde muchas veces ese acceso no es obvio. Cabe así mencionar, dentro de los datos personales a que pueden acceder las aplicaciones, los relativos a localización, contactos, identificadores únicos del dispositivo y del cliente (IIEM; IIAM; IUD y número de teléfono móvil), identidad del interesado, identidad del teléfono (los usuarios tienden a llamar a su móvil con su verdadero nombre) registros de llamadas, SMS y mensajería instantánea, historial de navegación, correo electrónico, fotografías y vídeos, credenciales de autenticación para los servicios de la sociedad de la información, datos biométricos (en modelos de reconocimiento facial y huellas dactilares), etc.

Asimismo los usuarios deben ser informados en un lenguaje claro y sencillo de si los datos pueden ser reutilizados por terceras partes, por ejemplo, los proveedores de análisis, en este caso cuando actúan exclusivamente en nombre del proveedor y no procesan datos para sus propios fines actúan como encargados del tratamiento, siendo exigible el contrato del artículo 12 de la Ley Orgánica 15/1999. Si utilizan los datos para sus propios fines actúan como responsables y precisan del consentimiento del interesado para tal tratamiento.

El grupo de trabajo también recomienda que los desarrolladores de aplicaciones incluyan en su política de privacidad información sobre cómo se ajusta la aplicación a la normativa europea de protección de datos, incluidas las posibles transferencias de datos personales a países que no son miembros del espacio económico europeo.

Igualmente recuerda que el consentimiento solamente es válido si la persona ha sido previamente informada sobre los principales elementos del tratamiento de datos, por lo que facilitar dicha información únicamente después de que el tratamiento de datos personales se haya iniciado carece de validez jurídica.

Estas recomendaciones derivan de la obligación establecida en el artículo 6 de la directiva de que los datos sean tratados de manera leal y lícita, obligación que en el Derecho Español se traduce en la prohibición contenida en el artículo 4.7 de la Ley Orgánica 15/1999 de recoger los datos por medios fraudulentos, desleales o ilícitos.

En cuanto a la forma, señala el aludido dictamen 02/2013 que la información debe estar a disposición de los usuarios antes de instalar la aplicación y debe seguir siendo accesible dentro de la aplicación tras su instalación. El grupo de trabajo del 29 recomienda que la información esté también disponible y fácilmente localizable por ejemplo dentro de la tienda de aplicaciones y preferiblemente en los sitios web del desarrollador responsable de la aplicación. Por otra parte teniendo en cuenta las limitaciones que puede presentar la cantidad de información que puede presentarse en una pantalla pequeña, el grupo recomienda que la información se facilita por capas, así en un primer aviso se facilita la información mínima exigible conforme al marco jurídico español y se pone a disposición del interesado información complementaria a través de enlaces al conjunto de la política de privacidad.

Debe, por otra parte, hacerse una referencia a la nueva regulación, aplicable a partir del 25 de mayo de 2018, ya que el Reglamento (UE) 2016/679 (Reglamento general de protección de datos) impone mayores exigencias respecto de la información que debe facilitarse a los interesados, lo que deberá tenerse en cuenta si el proyecto se sigue ejecutando con posterioridad a tal fecha, adaptando el formulario en que se recoja la información o la información que se facilite a los usuarios de la aplicación a tales exigencias.

El Reglamento General de protección de datos, incide especialmente en el principio de tratamiento lícito y leal de los datos personales. Señala el considerando 39 del aludido Reglamento que *"Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida."*

El artículo 13 de dicho Reglamento regula la información que debe facilitarse cuando los datos personales se obtengan del interesado, disponiendo lo siguiente:

"1.Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a *la identidad y los datos de contacto del responsable y, en su caso, de su representante;*

b *los datos de contacto del delegado de protección de datos, en su caso;*

c *los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento*

d *cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;*

e *los destinatarios o las categorías de destinatarios de los datos personales, en su caso;*

f *en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.*

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a *el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;*

b *la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;*

c *cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el*

consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d *el derecho a presentar una reclamación ante una autoridad de control;*

e *si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;*

f *la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.*

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información."

Por último, debe recordarse que el consentimiento 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. En el caso de la aplicación debe ser posible su desinstalación.

- Dentro de las obligaciones del responsable debe destacarse, en tercer lugar, el deber de implantar en el fichero o ficheros creados las debidas medidas de seguridad. Esta obligación incumbe igualmente a los encargados del tratamiento establecidos en España, tal y como dispone la Directiva 95/46/CE y el aludido Reglamento de desarrollo de la Ley Orgánica 15/1999.

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.

Por ello y sin perjuicio de las medidas de seguridad establecidas en el Reglamento de desarrollo de la Ley Orgánica 15/1999 que deben implantarse en todos los ficheros o tratamientos de datos personales que resulten de las actividades del proyecto, cabe hacer las siguientes consideraciones respecto de la seguridad en el caso de la aplicación que va a desarrollarse en el proyecto. Así deben tenerse en cuenta, en primer término, los principios de privacidad por defecto y desde el diseño, lo cual exige la evaluación continua de los riesgos actuales y futuros para la protección de datos y la aplicación de medidas correctoras eficaces.

En este sentido, y siguiendo nuevamente lo indicado por el grupo de trabajo del artículo 29 en el dictamen 02/2013, cabe mencionar que los desarrolladores de aplicaciones deben diseñar un entorno favorable a la seguridad, con herramientas que impidan la propagación de aplicaciones maliciosas y permitan la instalación y la desinstalación sencilla de la aplicación.

Señala el grupo de trabajo del artículo 29 entre las buenas prácticas que pueden aplicarse durante el diseño de una aplicación *"las relativas a la minimización de las líneas y la complejidad del código, y la aplicación de controles para excluir que los datos puedan transferirse o comprometerse involuntariamente. Además, deberían validarse todas las entradas para evitar desbordamientos de búfer o ataques de inyección. Otros mecanismos de seguridad que cabe destacar son la adecuación de las estrategias de gestión de los parches de seguridad y la realización de auditorías independientes de seguridad del sistema. Igualmente menciona que se debe alentar a los usuarios, mediante advertencias a complementar esas buenas prácticas de diseño con prácticas de usuario adecuadas como la actualización de sus aplicaciones con las últimas versiones disponibles, y recordatorios para evitar el uso repetido de contraseñas en los distintos servicios.*

Durante la fase de diseño de la aplicación, los desarrolladores también deben tomar medidas para evitar el acceso no autorizado a datos personales, garantizando la protección de datos tanto en tránsito como, en su caso, almacenados.

Las aplicaciones móviles deben funcionar en puntos específicos de la memoria de los dispositivos (separados por «aislamiento de procesos»), con objeto de reducir las consecuencias de los programas y las aplicaciones maliciosas. Los desarrolladores de aplicaciones deben utilizar, en estrecha colaboración con los fabricantes de sistemas operativos y las tiendas de aplicaciones, los mecanismos disponibles que permitan a los usuarios ver qué datos se están tratando en qué aplicaciones, y permitirles activar o desactivar de manera selectiva los correspondientes permisos. El uso de funciones ocultas no debe estar autorizado.

Los desarrolladores de aplicaciones deben considerar atentamente sus métodos de identificación y acreditación del usuario. No deben utilizar identificadores persistentes (específicos de los dispositivos) sino, por el contrario, usar identificadores de baja entropía específicos de cada aplicación o identificadores temporales del dispositivo, con objeto de evitar el seguimiento de usuarios a lo largo del tiempo. Debería considerarse el uso de mecanismos de autenticación más respetuosos de la intimidad. Al autenticar a los usuarios, los desarrolladores de aplicaciones deben prestar especial atención a la gestión de los códigos de identificación y las contraseñas de los usuarios. Estas últimas deben almacenarse cifradas y de forma segura, como un valor criptográfico de comprobación aleatoria cifrado. Además, al seleccionar identificadores de sesión, deben utilizarse series imprevisibles, posiblemente en combinación con información contextual como la fecha y la hora, además de la dirección IP o los datos de geolocalización.

La responsabilidad de los desarrolladores de aplicaciones en cuanto a la seguridad de sus productos no termina con la puesta en el mercado de una versión operativa. Las aplicaciones, como cualquier producto de software, pueden sufrir deficiencias de seguridad y tener puntos vulnerables, por lo que los desarrolladores deben elaborar soluciones o parches para los mismos y suministrárselos a aquellas partes que pueden ponerlas a disposición de los usuarios o hacerlo ellos mismos."

Debe igualmente 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 (esto es, en el caso español a la Agencia Española de protección de datos), disponiendo al respecto 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."

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, en tal caso no será preciso el consentimiento del interesado, en tanto no se produce una cesión de datos. 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.

A esta figura del encargado del tratamiento debe igualmente acudirse cuando una entidad que no tenga la condición de participante en el proyecto, realice alguna actividad para el mismo que comporte el tratamiento de datos personales, así, a título de ejemplo, una entidad que preste servicios de cloud computing o el denominado en la documentación aportada proveedor del servicio de la aplicación. Para que quienes presten estos servicios tengan tal condición de encargado del tratamiento, si el responsable está sujeto a la normativa de protección de datos española, será preciso que se dé cumplimiento a los requisitos exigidos por el artículo 12 de la Ley Orgánica 15/1999 y su normativa de desarrollo, en otro caso, como reiteradamente se ha señalado nos encontraríamos ante una cesión de datos que requeriría el consentimiento del interesado.

Igualmente, 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.

En el presente supuesto se señala que los datos recolectados sólo deben ser consultados por los investigadores que participan en el estudio y se recomienda el uso de una herramienta para almacenar y compartir datos que según se indica se encuentra alojada en España, desconociéndose respecto de la misma quien es el responsable, no obstante, debe tenerse en cuenta, que aunque no se lleven a cabo transferencias internacionales de datos, si resulta de aplicación lo señalado respecto del encargado del tratamiento.

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. Debe igualmente resaltarse que en el caso de la aplicación incluida en el proyecto, la finalidad debe estar bien definida y ser comprensible para un usuario medio sin conocimientos jurídicos o técnicos especiales.

La limitación de la finalidad está vinculada al principio de proporcionalidad, consagrado en el artículo 4.1 de la Ley Orgánica 15/1999 conforme al cual *"Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido."*

De este modo solamente deberán recabarse aquéllos datos que sean precisos para llevar a cabo las actividades objeto del proyecto. Dicho principio

tiene una especial incidencia en lo que respecta a la aplicación para móviles a utilizar en el proyecto, dado que, como se ha señalado, son muchos los datos contenidos en un terminal móvil al que las aplicaciones puede acceder, debiendo solicitarse el acceso y accederse solamente a los datos estrictamente necesarios para el funcionamiento de la aplicación. Esta limitación al acceso a datos forma parte igualmente de los principios de privacidad por defecto y desde el diseño.

Igualmente, dentro de los principios de calidad recogidos en la Ley Orgánica 15/1999, debe hacerse referencia al relativo a la conservación de los datos, disponiendo el número 5 del citado artículo 4 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. De la documentación aportada en el presente proyecto no se desprende una previsión en este sentido, no obstante, en aplicación de lo previsto en el artículo 4.5 arriba transcrito, deberá procederse a la cancelación de los datos personales una vez que no sean precisos para las finalidades para las que se recabó el consentimiento de los interesados.