N/REF: 328513/2016

Se solicita de la Agencia Española de Protección de Datos una aprobación ética para el tratamiento de datos personales que pudieran efectuarse en el marco de las actividades de investigación del proyecto europeo WYRED (netWorked Youth Research for Empowerment in the Digital Society), incluido en el ámbito del programa Horizonte 2020 de la Unión Europea.

El proyecto, según se señala en la documentación aportada, tiene como objetivo proporcionar un marco para la investigación en el cual los niños y jóvenes puedan expresar y explorar sus perspectivas e intereses en relación con la sociedad digital, pero también una plataforma desde la cual puedan comunicar sus perspectivas a otros actores de manera efectiva a través de procesos de compromiso innovadores. El proyecto se basa en el reconocimiento de que los jóvenes de todas las edades tienen derecho a la participación y al compromiso y tiene un enfoque de inclusión, diversidad y empoderamiento de los marginados.

En el marco de dicho proyecto se van a tratar datos especialmente protegidos. Asimismo se va a desarrollar una plataforma basada en la web y una aplicación para móviles, la plataforma permite la integración con redes sociales.

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

I

Con carácter previo debe señalarse que esta Agencia carece de competencia para emitir aprobaciones éticas. No obstante, viene atendiendo las peticiones de informes que le dirigen los responsables de los ficheros a los efectos de facilitarles el conocimiento y la interpretación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, evitando así incumplimientos involuntarios de la legislación vigente. En el

marco de esta actividad cabe examinar si los tratamientos de datos personales al que el proyecto objeto de consulta se refiere, que vayan a ser realizados por las entidades sujetas a la normativa de protección de datos española, son conformes a lo previsto en la citada Ley Orgánica 15/1999.

II

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.

A este respecto debe indicarse que los artículos 1 y 2 de la Ley Orgánica 15/1999, extienden su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento de sus datos de carácter personal, siendo definidos éstos en el artículo 3.a) de la citada Ley como "*cualquier información concerniente a personas físicas identificadas o identificables."*

El artículo 5.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999, 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».*

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, tras poner de manifiesto que la Directiva maneja un concepto lato de datos personales, analiza los elementos de dicha definición, señalando respecto a la expresión "toda información" 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».*

Debe, además resaltarse 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."* Por consiguiente, la imagen de las personas, si la calidad de la imagen permite su identificación, constituye un dato personal aunque no se encuentre asociada a ninguna otra información identificativa.

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 el proyecto, lo que incluye no solamente aquellos datos relativos a los menores, sino también los de los padres que firman el consentimiento en nombre de sus hijos menores de 18 años, y los de quienes de alguna manera participen en las actividades previstas en el proyecto.

Asimismo, desde el punto de vista de datos a tratar debe tenerse en cuenta que no solamente serán datos personales los mencionados en la consulta, sino las direcciones IP, los datos de localización, imágenes o voz de los usuarios identificados o identificables, etc. que pudieran captarse con la utilización de los recursos que el proyecto prevé poner a disposición de los usuarios. El tratamiento de todos estos datos personales quedará sujeto a lo establecido en la normativa de protección de datos personales.

En este sentido, debe hacerse referencia a la diferencia entre un proceso de seudonimización y un proceso de disociación, ya que éste último determina la inaplicación de la normativa de protección de datos. La Ley Orgánica 15/1999 describe éste último 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"*

En lo que respecta a la seudonimización cabe recordar que el aludido Grupo de Trabajo del Artículo 29, en su Dictamen 5/2014 sobre técnicas de anonimización, define la seudonimización como "la sustitución de un atributo (normalmente un atributo único) por otro en un registro" señalando que "por consiguiente, sigue existiendo una alta probabilidad de identificar a la persona física de manera indirecta; en otras palabras, el uso exclusivo de la seudonimización no garantiza un conjunto de datos anónimo. La seudonimización reduce la vinculabilidad de un conjunto de datos con la identidad del interesado; se trata, por tanto, de una medida de seguridad útil, pero no es un método de anonimización."

En este sentido señalaba el Dictamen 4/2007 del Grupo de Trabajo del artículo 29 respecto de un mecanismo de seudonimización habitual como son los datos cifrados que "Los datos cifrados son un ejemplo clásico de «*seudonimización*». La información contenida en esos datos se refiere a un individuo al que se asigna un código cifrado, mientras que la clave para descifrarlos, es decir para establecer la correspondencia entre el código y los identificadores habituales de la persona (nombre, fecha de nacimiento, dirección, etc.) se guardan por separado."

Así, a título de ejemplo, indicaba el Dictamen 4/2007 que "Si a cada persona física se le ha asignado un único código, siempre existe un riesgo de

identificación en caso de que sea posible acceder a la clave utilizada para el cifrado. Por lo tanto, los riesgos de un acceso ilegal desde el exterior, la probabilidad de que alguien de la organización remitente - a pesar de estar sujeto al secreto profesional -proporcione la clave *y por ende* la vía para una identificación indirecta, son factores que deben tenerse en cuenta para determinar si las personas pueden ser identificadas teniendo en cuenta el conjunto de medios que puedan razonablemente ser utilizados por el responsable del tratamiento o por cualquier otra persona y, por lo tanto, si la información debe considerarse como «datos personales».

El concepto de seudonimización aparece expresamente recogido en el artículo 4.5) del Reglamento europeo que define la «seudonimización» como "*el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable"*

El considerando 26 de dicho Reglamento recuerda que *"*Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos."

Y en el considerando 28, viene a poner de manifiesto la diferencia entre anonimización y seudonimización al señalar que "La *aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos."*

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.

De este modo, si la información relativa a las personas se encuentra asociada a un seudónimo, esta operación de seudonimización, por sí misma, no constituye un procedimiento de disociación puesto que a partir de la información de que se tiene conocimiento será posible realizar la operación inversa a la seudonimización, lo que da lugar a que la aplicación de la normativa de protección de datos no quede excluida.

En la consulta se señala que los participantes en la plataforma tendrán una identidad anónima que se elige al entrar en el proyecto y que se encontrará vinculada a los datos contenidos en una base de datos off line que será accesible solamente para un limitado número de miembros de personal del proyecto.

Por consiguiente, si bien la medida de seudonimización que se adopta en el proyecto debe valorarse positivamente en tanto contribuye, tal y como señala el Reglamento Europeo a reducir los riesgos para los interesados teniendo en cuenta muy especialmente que se trata de menores, no supone la inaplicación de la normativa de protección de datos a los datos contenidos en la plataforma, puesto que no se produce una efectiva anonimización. A ello debe añadirse que la interacción de las personas a través de la red social puede dar lugar a su identificación o que ellos mismos pueden aportar datos que les identifiquen. Ello puede ocurrir con la subida de materiales como fotos, videos, audios, comentarios, uso de servicios de mensajería internos, pero también a través de vínculos a otras redes sociales o incluso a partir de las relaciones que se establezcan entre las personas en la red.

Así, a modo de ejemplo, se encontrarán identificadas aquellas personas cuya imagen, con la suficiente resolución como para discernir sus rasgos faciales, aparezca en la red social, pero igualmente, puede dar lugar a la identificación de las personas la combinación de otro tipo de datos que, aparentemente o aisladamente, no parecen permitir dicha identificación. En este sentido el grupo de trabajo del 29 en el citado Dictamen 5/2014 recordaba que se ha demostrado que es posible extraer información sensible de personas concretas a partir de los gráficos de redes sociales, a pesar de las técnicas de seudonimización aplicadas a estos datos, ya que las relaciones entre personas son únicas y pueden utilizarse como identificadores

Debe así recordarse el 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.

De este modo constituirán tratamientos de datos personales no solamente aquellas operaciones que se lleven a cabo con los datos contenidos en la base de datos off line a que la consulta se refiere, sino igualmente las que pudieran efectuarse en la plataforma en la medida en que no existe una anonimización de los datos que en ella se traten.

III

Teniendo en cuenta la próxima entrada en vigor del Reglamento General de Protección de datos, debe hacerse referencia al mecanismo constituido por las evaluaciones de impacto que regula en su artículo 35 al disponer que "1.*Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares."*

Aunque la realización de una evaluación de impacto no sea exigible con anterioridad a la aplicabilidad del Reglamento europeo, debe tenerse en cuenta que puede serlo posteriormente, en particular si la ejecución del proyecto se prolonga hasta después de que este sea aplicable y en tanto se pretende mantener la plataforma con posterioridad a la vigencia del proyecto, por lo que puede ser recomendable efectuar esta evaluación teniendo en cuenta los diversos factores que aconsejarían efectuar la misma, entre ellos que el presente proyecto comporta el tratamiento de datos de menores de edad, se tratan categorías especiales de datos (tales como los relativos a religión o discapacidad) y que el tratamiento se lleva a cabo a utilizando nuevas tecnologías y a gran escala (participan diversos países europeos). A efectos de facilitar el análisis de riesgos y la adopción de medidas para mitigarlos o

eliminarlos que la evaluación de impacto comporta cabe tener en cuenta la guía de evaluación de impacto adoptada recientemente por el Grupo de Trabajo del Artículo 29, que puede consultarse en (http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083)

IV

Teniendo en cuenta que en el proyecto participan entidades españolas y de otros Estados miembros de la Unión Europea, así como terceros países no perteneciente a ésta, debe considerarse cuál es la normativa aplicable hasta tanto se produzca la aplicación del Reglamento Europeo.

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 (data controller y data processor respectivamente). 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."*

La figura del encargado del tratamiento 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.*"

Por consiguiente 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. 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.

V

En la presente consulta, la entidad española participante parece ostentar la condición del responsable del fichero off line que contiene los datos de los participantes, en tanto se señala la sujeción de dicho fichero a lo previsto en la Ley Orgánica 15/1999, desconociéndose si resulta igualmente responsable de la plataforma y de los posibles tratamientos de datos que en ella se lleven a cabo. En lo que respecta a las obligaciones impuestas por la Ley Orgánica 15/1999 al responsable 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.

- 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. En lo que respecta a datos especialmente protegidos, cabe recordar que el artículo 7 de la Ley Orgánica 15/1999 prevé un régimen especial para su tratamiento y cesión, disponiendo que:

"2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente."

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, a los que debe añadirse la característica de expreso en el caso de los datos a que se refiere el artículo 7.3 y expreso y por escrito cuando se trata de los datos a que hace referencia el artículo 7.2.

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 lo que respecta al consentimiento expreso, cabe recordar que la Sentencia de la Audiencia Nacional de 24 de marzo de 2006 señalaba lo siguiente: "Por consentimiento expreso hemos de entender aquél que se obtiene de una declaración clara e inequívoca por parte del interesado que acepta o rechaza la cesión y uso de sus datos mediante la expresión de su voluntad de forma que permita su constancia y prueba indubitada. La existencia de consentimiento expreso, referido a la cesión y uso de estos datos especialmente sensibles no debe admitir duda ni entenderse o interpretarse en varios sentidos, o poder dar ocasión a juicios diversos"

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 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.

Mención especial merece el tratamiento de los datos de los menores que vayan a participar en el proyecto. El Reglamento de desarrollo de la Ley Orgánica 15/1999, aplicable en la actualidad fija la edad de 14 años como edad mínima para prestar el consentimiento en su artículo 13.1, según el cual *"1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores."*

El Reglamento Europeo, en su artículo 8 exige una edad mínima de 16 años para que los menores puedan consentir el tratamiento de sus datos cuando se trata de servicios de la sociedad de la información. No obstante permite que los Estados miembros puedan establecer por Ley a tales fines una edad inferior, que no sea menor a la de 13 años. En el presente proyecto se exigirá el consentimiento de los padres para los tratamientos de datos de los menores de 18 años participantes, lo que permite un tratamiento uniforme

dentro del proyecto para todos los menores participantes cualquiera que sea el país de origen y el desarrollo legal que en el mismo se lleve a cabo.

Por otra parte, el aludido artículo 13.4 del Reglamento de desarrollo de la Ley Orgánica 15/1999 establece que *"Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales."*

En el presente supuesto, se hace referencia a que el consorcio desarrollará un procedimiento de consentimiento con diferentes versiones en función de la edad del individuo y la capacidad de firmar el documento, procedimiento que deberá tener en cuenta los requerimientos que se han venido señalando. Debe tenerse en cuenta que tanto la prestación del consentimiento como el cumplimiento del deber de información deberán poder ser acreditados por el responsable del fichero o tratamiento. Dispone a estos efectos el artículo 12.3 del Reglamento de desarrollo de la Ley Orgánica 15/1999, que "*corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.*" De la misma manera, tras la anulación de lo previsto en el artículo 18 del mismo Reglamento por Sentencia de 15 de julio de 2010 del Tribunal Supremo, debe entenderse que rige igualmente la libertad de forma para acreditar el cumplimiento del deber de información, de modo que el responsable podrá demostrar por cualquier medio de prueba admisible en derecho el cumplimiento de ambos deberes.

Por otra parte, debe determinarse quién es el responsable de la plataforma, de los tratamientos de datos que en ella se efectúen y en consecuencia, ante quien pueden ejercitarse los derechos que reconoce la normativa de protección de datos. Deberá así implementarse un procedimiento que permita tal ejercicio teniendo en cuenta que los datos de los participantes se encuentran seudonimizados y que, al menos en lo que a la normativa española respecta, el procedimiento establecido en el Reglamento de desarrollo de la Ley Orgánica 15/1999 exige la identificación del titular de los datos para ejercitar tales derechos.

En el caso de que el proyecto desarrolle una aplicación para móviles para acceder a la plataforma, debe tenerse en cuenta que el Grupo de Trabajo del artículo 29 en su informe 02/2013 sobre las aplicaciones de los dispositivos inteligentes señala 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 lo que respecta a la aplicación para móviles resulta especialmente importante la información sobre qué datos se están tratando 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.

El Grupo de Trabajo del artículo 29, recuerda respecto de los datos que van a ser objeto de tratamiento con la aplicación 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.

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."

- 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. Las medidas de seguridad a adoptar en el presente supuesto serán las de nivel alto, en tanto se tratan datos especialmente protegidos, lo que implica, de conformidad con lo previsto en el artículo 81 de dicho Reglamento, que implementen también las exigibles para niveles de seguridad inferiores.

Sin perjuicio de la adopción de las debidas 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, en el caso de que se desarrolle una aplicación debe tenerse en cuenta lo señalado por el Grupo de Trabajo del artículo 29 el dictamen 02/2013, respecto a la necesidad de que los desarrolladores de aplicaciones diseñen 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. Así deben tenerse en cuenta 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.

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."

VI

Si las entidades sujetas a la normativa de protección de datos española efectuasen una comunicación en cualquier forma, incluida la visualización, de los datos personales a terceros, entre los que se encuentran las demás

entidades participantes en el proyecto, dicha comunicación 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.

En lo que respecta a la posibilidad mencionada en el proyecto de acceso a los datos por terceros, por ejemplo investigadores, dentro del contexto de una política de open data, señalando que solamente serán datos accesibles los datos anonimizados, cabe recordar igualmente 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."*

De otra parte, en la política de uso de la plataforma que se establezca, resulta recomendable dar información clara a los participantes sobre cómo actuar para proteger su privacidad y la de terceros a fin de salvaguardar en lo posible el proceso de seudonimización y evitar que se produzcan incumplimientos de la normativa de protección de datos, como la libre difusión de imágenes de terceros sin contar con el consentimiento de éstos.

VII

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 en los términos vistos.

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. 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

En lo que respecta al mantenimiento de la plataforma después de la finalización del proyecto, se carece de datos para pronunciarse, desconociéndose incluso quien es el responsable de la misma, no obstante, si el responsable o responsables tuviesen establecimiento en España, estarán sometidos a lo dispuesto en la Ley Orgánica 15/1999 en la forma señalada en el presente informe o a lo previsto en el 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), en el momento en que este resulte aplicable.

VIII

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".*

No obstante, el artículo 34 de la misma Ley señala que lo dispuesto en el artículo anterior no será de aplicación: "*k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado."* 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.

Así, 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."*

En lo que a Turquía respecta, en tanto no existe una decisión que declare que un nivel de adecuado de protección la autorización de transferencia internacional de datos podría otorgarse si se obtienen garantías suficientes. Así, podrá ser otorgada si el responsable del fichero aporta un contrato escrito, celebrado entre el exportador y el importador de datos, en el que consten las necesarias garantías de respeto a la protección de la vida

privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

Esta Agencia ha venido señalando que cuando la transferencia internacional de datos se lleve a cabo entre responsables del tratamiento, se considerará que reúnen las garantías adecuadas los contratos celebrados en los términos previstos en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de junio de 2001, y 2004/915/CE, de 27 de diciembre de 2004, por la que se modifica la anterior. Cuando la transferencia de datos se realice entre un responsable y un encargado del tratamiento se considerarán que reúnen las garantías adecuadas los contratos que incluyan las cláusulas contractuales tipo establecidas en la Decisión de la Comisión Europea 2010/87/UE, de 5 de febrero de 2010.

El procedimiento para obtener la autorización para efectuar transferencias basadas en alguna de las cláusulas contractuales tipo citadas se encuentra regulado en los artículos 137 y siguientes del Reglamento de desarrollo de la Ley Orgánica 15/1999. Ahora bien, dadas las dificultades que tal procedimiento puede ocasionar, debe examinarse si se van a transferir efectivamente datos personales al país tercero y, en tal caso, analizar si cabe aplicar aquí la excepción prevista en el artículo 34 e) de la Ley Orgánica 15/1999 referida a que *"el afectado haya dado su consentimiento inequívoco a la transferencia prevista"* en cuyo caso no sería preciso solicitar tal autorización del Director de la Agencia Española de Protección de Datos. El modelo de solicitud de consentimiento puede incorporar dicho extremo permitiendo al interesado denegar o aceptar tal transferencia de datos. Debe no obstante recordarse que la transferencia internacional de datos deberá ser notificada al Registro General de Protección de datos, tal y como dispone el artículo 66.3 del Reglamento de desarrollo de la Ley Orgánica 15/1999, antes transcrito. Dicha notificación puede llevarse a cabo en el momento de inscripción del fichero o, si ya estuviese inscrito, en una posterior modificación, indicando el país o países que recibirán la transferencia de datos personales y detallando en la misma que tal transferencia se va a amparar en lo previsto en el artículo 34 e) de la Ley Orgánica 15/1999.

IX

Debe hacerse una referencia a la necesidad de considerar donde se alojan los datos personales que se tratan en la plataforma, especialmente si se incorporan a un servicio de cloud computing, se alojan copias de seguridad en servidores situados fuera del espacio económico europeo, etc. En el supuesto de que el responsable esté sujeto a la normativa de protección de datos española, además de la necesidad de firmar el contrato a que se refiere el artículo 12 de la Ley Orgánica 15/1999, si tales servicios se contratan con un tercero, podemos encontrarnos con transferencias internacionales de datos que, en caso de que el país en que se encuentren no cuente con una decisión

de la Comisión de la Unión Europea que declare que existe un nivel adecuado de protección, exigirán la prestación de las correspondientes garantías.

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

Ahora bien, como indica el grupo de trabajo del artículo 29 en el Dictamen 5/2012 sobre la computación en nube "En la actual situación de la computación en nube, los clientes de estos servicios pueden no tener margen de maniobra a la hora de negociar las condiciones de uso de los mismos, ya que las ofertas normalizadas son una característica de muchos servicios de computación en nube. No obstante, en última instancia, es el cliente quien decide sobre la asignación de parte o de la totalidad de las operaciones de tratamiento a los servicios en nube con fines específicos; la función del proveedor de estos servicios será la de contratista frente al cliente, que es el punto clave en este caso. Tal como se recoge en el Dictamen 1/2010 del GT 29 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», «*el desequilibrio en cuanto al poder contractual entre un pequeño responsable del tratamiento y un gran proveedor de servicios no debería considerarse una justificación para que el primero acepte cláusulas y condiciones de contratos que no se ajusten a la legislación en materia de protección de datos*». Por esta razón, el responsable del tratamiento debe elegir un proveedor que garantice el cumplimiento de la legislación sobre protección de datos"

En este sentido, debe tomarse en consideración lo señalado por esta Agencia en la guía publicada para facilitar el cumplimiento de la normativa de protección de datos a las entidades que contraten servicios de computación en nube, que se encuentra disponible en la página web (http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf). En el caso de que el responsable del fichero sea una Administración Pública debe tenerse en cuenta, como recuerda dicha guía, que las Administraciones Públicas, están sujetas, además de a la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y a su Reglamento de desarrollo, aprobado por Real Decreto 1720/20007, a un marco

legal específico al cual debe adecuarse la prestación de servicios basados en cloud computing, y que está constituida por la normativa vigente en materia de contratos del sector público y de Administración electrónica.

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

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

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

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

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

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

Añade que "*En ciertos casos, la complejidad de los servicios contratados puede aconsejar la designación de un responsable del contrato en los términos*

previstos en el artículo 52 del RDL 3/2011, de 14 de noviembre, con el fin de asegurar la correcta realización de la prestación pactada. No obstante, la designación de dicha figura no modifica el régimen de obligaciones y responsabilidades al que está sujeto el responsable del tratamiento en materia de protección de datos de carácter personal"

Asimismo la guía especifica las siguientes cuestiones:

"La prestación de servicios por encargados de tratamiento en cloud debería quedar claramente identificada en el documento de seguridad. Asimismo, el acceso a la información debe reunir un nivel de medidas de seguridad equivalente al de los accesos en modo local, en la forma dispuesta por el Título VIII del RLOPD.

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

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

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

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

• Incidentes de seguridad y continuidad de la actividad. La adopción de modelos de servicio basados en cloud computing debe contemplar una adecuada gestión de las incidencias de seguridad y mecanismos que garanticen la continuidad de las operaciones en caso de catástrofes o incidentes severos.

• Auditoría de la seguridad. La contratación de servicios de cloud computing exige garantizar la realización de las auditorías de seguridad

ordinarias y extraordinarias previstas en el artículo 34 del Esquema Nacional de Seguridad. Este artículo exige requisitos específicos sobre los criterios, métodos de trabajo y de conducta utilizados; los aspectos respecto de los que debe determinar la auditoría y los criterios metodológicos utilizados."

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

Debe tenerse en cuenta también, que, como consecuencia del encargo del tratamiento o de las sucesivas subcontrataciones, puede originarse una transferencia internacional de datos. En particular y en lo que respecta a los servicios de cloud computing indica el Dictamen 5/2012 del Grupo de Trabajo del artículo 29 que una de sus características es que "se basa a menudo en la total falta de ubicación estable de los datos en la red del proveedor. Los datos pueden encontrarse en un centro de datos a las 2 horas y en el otro lado del mundo a las 16 horas. Por tanto el cliente rara vez se encuentra en posición de saber en cualquier momento en que lugar están situados, almacenados o transferidos los datos." Señala así dicho Dictamen que la transparencia en la nube supone que es necesario que el cliente tenga conocimiento de todos los subcontratistas que contribuyan a la prestación de los respectivos servicios en nube, así como de la localización de todos los centros donde puedan tratarse los datos personales. Sólo entonces podrá evaluar si los datos personales pueden ser transferidos a un llamado tercer país fuera del Espacio Económico Europeo (EEE) que no garantice un nivel adecuado de protección en el sentido de la Directiva 95/46/CE.

En particular, en lo que respecta a las transferencias de datos personales a Estados Unidos, la decisión en la que se consideraba que existía un nivel de protección adecuado respecto de las entidades estadounidenses adheridas a los «principios de Puerto Seguro" ha sido anulada por la Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015, .asunto C-362/14. Shrems v Data Protection Commissioner. No obstante, la Comisión Europea ha adoptado en fecha 12 de julio de 2016 una nueva Decisión, debiendo apreciarse que existe un nivel adecuado de protección respecto de las entidades que se adhieran a los principios del ahora denominado "Privacy Shield", lo que deberá comprobarse en cada caso antes de proceder a la transferencia de datos personales.

Así pues, no sería precisa la autorización del Director de la Agencia Española de protección de Datos cuando la Comisión de la Unión Europea

haya considerado que en el país receptor existe un nivel de protección adecuado o, en el caso de Estados Unidos, respecto de las empresas adheridas a los principios de Privacy Shield para la prestación de los correspondientes servicios de cloud computing. Sin embargo, 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 anteriormente transcrito.

Por consiguiente, además de las específicas cuestiones señaladas respecto de la contratación para las Administraciones Públicas, medidas de seguridad y portabilidad, debe tenerse especialmente presente al contratar un servicio de cloud computing los aspectos relativos a la subcontratación y a las transferencias internacionales de datos y, en particular, en caso de que se produzcan transferencias de datos a EEUU debe comprobarse que los subcontratistas en dicho país están adheridas a los principios de Privacy Shield para la prestación de dichos servicios de cloud computing.