



Se consulta si resulta conforme a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, determinadas cláusulas de un contrato de prestación de servicios de cloud computing a la clínica médica consultante. El consultante se limita a transcribir el contenido de las cláusulas desconociéndose tanto que servicios van a contratarse de los proporcionados por el prestador del servicio de cloud computing como el tipo de datos que van a tratarse en dicho sistema.

Con carácter previo al examen de la conformidad de dichas cláusulas con la normativa de protección de datos española, debe hacerse una referencia general a las diversas cuestiones que plantea el servicio de cloud computing en materia de protección de datos personales, para ello va a tomarse como referencia 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 5/2012 sobre la computación en nube, cuyas conclusiones son de interés para la determinación de las condiciones de contratación del servicio.

El Grupo de Trabajo del artículo 29, analiza los riesgos específicos que puede generar el tratamiento de datos personales en la nube, dividiendo éstos en dos categorías: la falta de control sobre los datos y la falta de transparencia, esto es, la insuficiente información sobre la propia operación de tratamiento.

En lo que a la falta de control se refiere, señala el Dictamen aludido que “Al introducir datos personales en los sistemas gestionados por un proveedor, los clientes de servicios de computación en nube (en lo sucesivo, «clientes») pueden no seguir teniendo el control exclusivo de estos datos y no pueden aplicar las medidas técnicas y de organización necesarias para garantizar la disponibilidad, integridad, confidencialidad, transparencia, aislamiento, posibilidad de intervención y portabilidad de los datos. Esta falta de control puede manifestarse de la siguiente manera:

- Falta de disponibilidad debido a la falta de interoperatividad (dependencia respecto del proveedor): si el proveedor se basa en tecnología patentada, puede resultar difícil para un cliente mover los datos y documentos entre diferentes sistemas en la nube (portabilidad de los datos) o intercambiar información con entidades que utilicen servicios de computación en nube gestionados por distintos proveedores (interoperatividad).
- Falta de integridad causada por la puesta en común de los recursos: una nube se compone de sistemas e infraestructuras comunes. Los proveedores tratan datos personales procedentes de una amplia gama de interesados y organizaciones, y es posible que surjan conflictos de intereses u objetivos diferentes.

- Falta de confidencialidad por lo que respecta a las solicitudes de intervención legal realizadas directamente a un proveedor: los datos personales tratados en la nube pueden ser objeto de solicitudes de intervención legal por parte de las autoridades policiales o judiciales de los Estados miembros de la UE y de terceros países. Existe el riesgo de revelación de datos personales a servicios incluso extranjeros sin una base jurídica de la UE válida y, por tanto, se daría una violación de la legislación de la UE sobre protección de datos.
- Falta de posibilidad de intervención debido a la complejidad y la dinámica de la cadena de subcontratación: el servicio de computación en nube ofrecido por un proveedor puede realizarse combinando servicios de varios proveedores distintos, que pueden añadirse o suprimirse dinámicamente a lo largo de la duración del contrato del cliente.
- Falta de posibilidad de intervención (derechos de los interesados): un proveedor no podrá aportar las medidas e instrumentos necesarios para ayudar al responsable del tratamiento a gestionar los datos en términos de, por ejemplo, acceso, supresión o corrección.
- Falta de aislamiento: un proveedor podrá ejercer su control físico sobre los datos de distintos clientes para vincular los datos personales. Si se proporciona a los administradores derechos de acceso suficientemente privilegiados (funciones de alto riesgo), podrían vincular información de distintos clientes. “

En lo que atañe a la falta de información sobre el tratamiento (transparencia) el Dictamen afirma que “La falta de información sobre las operaciones de tratamiento de un servicio de computación en nube plantea un riesgo para los responsables del tratamiento y para los interesados, que pueden no ser conscientes de las amenazas y riesgos potenciales y por tanto no podrán adoptar las medidas que consideren apropiadas. Algunas posibles amenazas pueden derivarse de que el responsable del tratamiento no sepa que:

- Se realiza un tratamiento en cadena con múltiples encargados del tratamiento y subcontratistas.
- Los datos personales se tratan en diferentes zonas geográficas del EEE. Ello incide directamente en la legislación de protección de datos aplicable a los litigios que puedan surgir entre usuario y proveedor.
- Se transmiten datos personales a terceros países no pertenecientes al EEE. Los terceros países pueden no proporcionar un nivel adecuado de protección de datos y las transferencias pueden no contar con las medidas de protección adecuadas (por ejemplo, cláusulas contractuales estándar o normas empresariales vinculantes) y, por tanto, esto puede ser ilegal.”

La entidad que contrata un servicio de cloud computing, debe considerar dichos riesgos, teniendo en cuenta que sigue siendo responsable del tratamiento de los datos personales, y que dicha responsabilidad no se desplaza al proveedor del servicio aunque sea una gran compañía multinacional o incorpore una cláusula al respecto. En cuanto a la normativa de protección de datos aplicable será la del país en que esté establecido el responsable del tratamiento que contrata los servicios de computación en nube y no la del lugar en que se encuentren los proveedores de dichos servicios. Por su parte, los proveedores de dichos servicios tendrán la condición de encargados del tratamiento, definidos en la Ley Orgánica 15/1999 como *“la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento”*. El Reglamento de desarrollo de la Ley Orgánica precisa esta definición especificando en su artículo 5.1.i) que el encargado del tratamiento será *“La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.”*

La relación entre responsable del fichero o tratamiento, en el presente caso la clínica consultante, y el encargado, en el presente caso la entidad prestadora de servicios de cloud computing, deberá formalizarse en un contrato en los términos establecidos por el artículo 12 de la Ley Orgánica 15/1999.

Ahora bien, como indica el Grupo de Trabajo del artículo 29 en el Dictamen a que se viene haciendo referencia *“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 aludido Grupo de Trabajo del artículo 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”

De ahí que en dicho Dictamen se señale que las empresas que deseen utilizar la computación en nube deben efectuar, como primer paso, un análisis de riesgos completo y riguroso, teniendo en cuenta su condición de responsable del tratamiento. El Dictamen les recomienda que seleccionen un proveedor de servicios



de cloud computing que garantice el cumplimiento de la legislación sobre protección de datos, y que verifiquen si el proveedor de tales servicios puede garantizar la legalidad de las transferencias internacionales de datos. Debe así tenerse en cuenta, que como pone de relieve el Grupo de Trabajo del artículo 29 internacional de Berlín sobre protección de datos en las telecomunicaciones, en el Memorándum Sopot adoptado en 2012, en el que se analizan cuestiones relativa a la intimidad y protección de datos en la computación en nube, ésta no debe conducir a una disminución de los niveles de protección de datos en comparación con el tratamiento convencional

II

En lo que respecta a las cuestiones concretas formuladas por el consultante, se plantea en primer lugar si la cláusula del contrato que transcribe en la consulta, es suficiente para dar cumplimiento a lo previsto en el artículo 12 de la Ley Orgánica 15/1999.

Dispone el artículo 12 de la Ley Orgánica 15/1999 “2.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.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. 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.

4. 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.”

En la cláusula transcrita por el consultante no se especifican ni los servicios a prestar ni se determinan las instrucciones del cliente, ni se señalan ninguno de los otros aspectos recogidos en dicho precepto, limitándose a indicar con carácter genérico que se tratarán los datos personales del cliente de conformidad con sus instrucciones. De otra parte dichas instrucciones se subordinan a las capacidades y a la política de privacidad del proveedor del servicio, indicándose simplemente que cuando el proveedor considere que entran en conflicto lo pondrá en conocimiento del



cliente tan pronto como sea razonablemente factible, que tras la notificación podrá resolver el contrato, debiendo notificarlo por escrito al proveedor.

Por consiguiente, dicha cláusula resulta insuficiente a efectos de lo establecido en el artículo 12 de la Ley Orgánica 15/1999, debiendo especificarse todas aquellas cuestiones que, para dar cumplimiento a lo establecido en la normativa de protección de datos, sean exigibles por parte del consultante teniendo en cuenta el tipo de datos cuyo tratamiento vaya a efectuarse en la nube y los servicios a prestar por el proveedor del dicho servicio.

A título ilustrativo cabe transcribir aquí los aspectos que, enumerados por el Grupo de Trabajo del artículo 29 en el aludido Dictamen 5/2012, deben concretarse en el contrato.

- Datos sobre el alcance y las modalidades de las instrucciones del cliente que deberán darse al proveedor, con especial atención a los acuerdos sobre nivel de servicios aplicables (que deberán ser objetivos y mensurables) y las sanciones correspondientes (financieras o de otro tipo, incluida la posibilidad de demandar al proveedor en caso de incumplimiento).
- Especificación de las medidas de seguridad que deberá cumplir el proveedor, en función de los riesgos que presente el tratamiento y la naturaleza de los datos que deban protegerse.

A este respecto menciona el Dictamen 5/2012 que deben garantizarse los objetivos esenciales de:

- Disponibilidad, esto es la garantía de acceso oportuno y fiable a los datos, señala así que una grave amenaza para la disponibilidad en la nube es la pérdida accidental de conectividad de red entre el cliente y el proveedor o del rendimiento de los servidores a causa de acciones malintencionadas tales como ataques de denegación del servicio. El responsable del tratamiento debe comprobar si el proveedor ha adoptado medidas razonables para afrontar el riesgo de perturbaciones, tales como copia de seguridad de los enlaces de internet, almacenamiento suplementario y mecanismos efectivos para la copia de seguridad de los datos.
- Integridad. La integridad puede definirse como la característica de que los datos son auténticos y no han sido maliciosamente o accidentalmente alterados durante el tratamiento, almacenamiento o transmisión. La noción de integridad puede ampliarse a los sistemas informáticos y exige que el tratamiento de datos personales en estos sistemas no se altere.

Pueden detectarse las alteraciones de datos personales mediante mecanismos de autenticación criptográfica tales como códigos de autenticación de mensajes o firmas. La interferencia con la integridad de los



sistemas informáticos en la nube puede prevenirse o detectarse mediante sistemas de prevención y detección de intrusiones (IPS/IDS). Esto es especialmente importante en el tipo de entornos de red abierta en que suelen operar las nubes.

- **Confidencialidad.** En el medio en nube, el cifrado puede contribuir de forma significativa a la confidencialidad de los datos personales si se aplica correctamente, aunque no anonimice de forma irreversible los datos personales (el cifrado no implica que no sean de aplicación las obligaciones de protección de datos). El cifrado de datos personales deberá utilizarse en todos los casos «en tránsito» y, cuando esté disponible, para los datos «en reposo» Este último, señala el Grupo de Trabajo del artículo 29, es el caso, en particular, de los responsables del tratamiento que prevén transferir datos sensibles en el sentido del artículo 8 de la Directiva 95/46/CE (por ejemplo, datos sobre la salud) a la nube o que están sujetos a obligaciones jurídicas específicas de secreto profesional. Señala asimismo, que en algunos casos (por ejemplo, un servicio de almacenamiento laaS) un cliente podrá no depender de la solución de cifrado propuesta por el proveedor y optar por cifrar los datos personales antes de enviarlos a la nube. Cifrar los datos en reposo exige prestar una atención especial a la gestión de las claves criptográficas, ya que la seguridad de los datos depende en última instancia de la confidencialidad de las claves de cifrado.

Las comunicaciones entre el proveedor y el cliente, así como entre los centros de datos, deberán estar cifradas. La administración remota de la plataforma en nube sólo deberá realizarse a través de un canal de comunicación seguro. Si un cliente prevé no sólo almacenar, sino también tratar datos personales en la nube (por ejemplo, búsqueda de bases de datos para los registros), deberá tener en cuenta que la codificación no puede mantenerse durante el tratamiento de los datos (con excepción de casos muy específicos). Otras medidas técnicas destinadas a garantizar la confidencialidad incluyen mecanismos de autorización y autenticación.

- **Aislamiento.** En las infraestructuras en nube, los recursos como el almacenamiento, la memoria y las redes son comunes a muchos arrendatarios. Esto crea nuevos riesgos de que los datos se revelen y traten con fines ilegítimos así como mantener la confidencialidad y la integridad.

Para lograr el aislamiento se requiere en primer lugar una gestión adecuada de los derechos y funciones para acceder a los datos personales, objeto de revisión regular. Debería evitarse establecer funciones con privilegios excesivos (por ejemplo, ningún usuario ni administrador debe ser autorizado a acceder al conjunto de la nube). De manera más general, los administradores y usuarios sólo deben poder acceder a la información que necesiten para sus fines legítimos (principio del mínimo privilegio). Menciona así el Grupo de Trabajo del artículo 29 también que se ofrezcan por el proveedor garantías para el registro y auditoría de las operaciones de



tratamiento de datos personales realizadas por los empleados del proveedor o los subcontratistas.

- Posibilidad de intervención. El cliente deberá verificar que el proveedor no impone obstáculos técnicos y de organización para que pueda darse cumplimiento a los derechos de acceso, rectificación, cancelación, oposición y a la supresión y bloqueo de los datos. El contrato entre el cliente y el proveedor deberá precisar que el proveedor está obligado a apoyar al cliente facilitando el ejercicio de los derechos de los interesados y a garantizar que lo mismo se aplica a su relación con los subcontratistas.
- Portabilidad. Actualmente, la mayoría de los proveedores no utiliza formatos de datos e interfaces de servicios estándar que facilitan la interoperatividad y la portabilidad entre los diferentes proveedores. Si un cliente decide migrar de un proveedor a otro, esta falta de interoperatividad puede dar lugar a la imposibilidad o al menos a dificultades para transferir los datos (personales) del cliente al nuevo proveedor (esto se denomina dependencia respecto al proveedor). Lo mismo ocurre con los servicios desarrollados por el cliente en una plataforma ofrecida por el proveedor original (PaaS). Antes de contratar un servicio de computación en nube, el cliente deberá comprobar si el proveedor garantiza la portabilidad de los datos y servicios y de qué manera lo hace. En cualquier caso, deberán acordarse cláusulas contractuales que estipulen formatos garantizados, la preservación de las relaciones lógicas y los costes derivados de la migración a otro proveedor.
- Responsabilidad. En informática, la responsabilidad puede definirse como la capacidad de determinar lo que hizo una entidad en un momento determinado en el pasado y de qué manera lo hizo. En el ámbito de la protección de datos, este concepto tiene a menudo un sentido más amplio y describe la capacidad de las partes para demostrar que tomaron las medidas adecuadas para garantizar la aplicación de los principios de protección de datos.

La responsabilidad en informática es especialmente importante para investigar violaciones de datos personales, en las que los clientes, proveedores y el subencargado del tratamiento pueden tener cada uno algún grado de responsabilidad operativa. La capacidad de la plataforma en la nube para proporcionar mecanismos de registro amplios y un control fiable es de vital importancia a este respecto.

Además, los proveedores deberán proporcionar pruebas documentales de la adopción de medidas adecuadas y efectivas que aporten los resultados de los principios de protección de datos señalados en las secciones anteriores. Son ejemplos de dichas medidas los procedimientos para garantizar la identificación de todas las operaciones de tratamiento de datos; para responder a las solicitudes de acceso; la asignación de recursos, etc.



- Supresión de datos. De conformidad con el artículo 6, apartado 1, letra e), de la Directiva 95/46/CE, los datos personales deberán ser conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los datos personales que ya no sean necesarios deberán suprimirse o anonimizarse. Si no pueden suprimirse debido a una obligación jurídica de conservarlos (por ejemplo, normas fiscales), el acceso a ellos deberá bloquearse. Es responsabilidad del cliente garantizar que los datos personales se supriman tan pronto como dejen de ser necesarios en el sentido mencionado.

El principio de supresión de datos se aplica a los datos personales con independencia de si están almacenados en un disco duro o en otros medios (por ejemplo, cintas de copia de seguridad). Dado que los datos personales pueden mantenerse de forma redundante en diferentes servidores en diferentes lugares, deberá garantizarse que todos ellos se supriman irreversiblemente (es decir, las versiones anteriores, ficheros temporales e incluso fragmentos de ficheros también deberán suprimirse). Los clientes deberán ser conscientes de que los datos de registro que facilitan la auditoría de, por ejemplo, el almacenamiento, la modificación o la supresión de datos, también pueden considerarse datos personales relativos a la persona que inició la operación de tratamiento en cuestión.

Garantizar la supresión de los datos personales exige que los medios de almacenamiento sean destruidos o desmagnetizados, o que los datos personales se supriman efectivamente grabando encima de ellos. Para esta sobreescritura, deberán utilizarse programas informáticos especiales que sobreescriban datos múltiples veces de conformidad con una especificación reconocida.

El cliente deberá asegurarse de que el proveedor garantice una supresión segura en el sentido mencionado y que el contrato entre el proveedor y el cliente contenga disposiciones claras relativas a la supresión de los datos personales. Lo mismo se aplica a los contratos entre proveedores y subcontratistas.

- Objeto y calendario del servicio de computación en nube que deberá prestar el proveedor, alcance, forma y finalidad del tratamiento de datos personales por el proveedor, así como tipos de datos tratados.
- Especificación de las condiciones necesarias para devolver los datos (personales) o destruirlos una vez finalizado el servicio. Además, debe garantizarse que los datos personales se borran con seguridad a petición del cliente.



- Inclusión de una cláusula de confidencialidad, vinculante tanto para el proveedor como para cualquiera de sus empleados que puedan tener acceso a los datos. Sólo las personas autorizadas podrán tener acceso a los datos.
- Obligación del proveedor de apoyar al cliente facilitando el ejercicio de los derechos de los interesados a acceder, rectificar o suprimir sus datos.
- Clarificación de las responsabilidades del proveedor en cuanto a notificación al cliente en caso de violaciones de datos que afecten a sus datos.
- El contrato deberá establecer expresamente que el proveedor no podrá comunicar los datos a terceros, ni siquiera con fines de conservación, a menos que el contrato prevea la existencia de subcontratistas, en la forma en que se verá en el siguiente epígrafe de este informe.
- Obligación del proveedor de proporcionar una lista de los lugares donde se tratarán los datos.
- Derecho del responsable del tratamiento a controlar, y la correspondiente obligación del proveedor de cooperar.
- Debe establecerse contractualmente que el proveedor deberá informar al cliente acerca de los principales cambios relativos a sus respectivos servicios, tales como la ejecución de funciones adicionales.
- El contrato deberá prever el registro y la auditoría de las operaciones de tratamiento de datos personales realizadas por el proveedor o los subcontratistas.
- Notificación al cliente de toda solicitud jurídicamente vinculante de divulgar datos personales presentada por las autoridades policiales o judiciales a menos que esté prohibido; por ejemplo, la prohibición en virtud del Derecho penal de mantener la confidencialidad de una investigación policial.
- Obligación general del proveedor de garantizar que su organización interna disposiciones de tratamiento de datos (y las de sus subcontratistas, en su caso) son conformes con las normas y los requisitos legales nacionales e internacionales aplicables.

Señala el Grupo de Trabajo del artículo 29 en el aludido Dictamen 5/2012 que cuando un responsable del tratamiento decida contratar servicios de computación en nube deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse y se asegure de que se cumplen dichas medidas. Ahora bien, dadas las dificultades que puede plantear al responsable del tratamiento la realización de auditorías para verificar dicho



cumplimiento, considera que la auditoría puede ser sustituida por la efectuada por un tercero de reconocido prestigio elegido por el responsable del tratamiento. Hace así referencia a una certificación emitida por un tercero de reconocido prestigio de la realización de una auditoría o revisión con respecto a una norma reconocida que cumpla los requisitos expuestos en el Dictamen 5/2012, e indica que tales normas incluyen las emitidas por la Organización Internacional de Normalización, el Consejo de Normas Internacionales de Auditoría y Aseguramiento y el Consejo de Normas de Auditoría del American Institute of Certified Public Accountants, en la medida en que estas organizaciones hayan establecido normas que cumplen los requisitos que figuran en el Dictamen. De este modo podría suplirse la realización de una auditoría por el responsable por una certificación siempre que ésta cubra tanto las medidas técnicas (tales como la localización de los datos o la codificación) como los procesos seguidos por los proveedores de servicios de computación en nube para garantizar la protección de los datos.

Esta solución ha sido igualmente considerada favorablemente por esta Agencia, en informe 157/2012 que puede consultarse en su página web, aunque la entidad auditora haya sido contratada por el proveedor del servicio, siempre y cuando la entidad auditora sea una entidad enteramente independiente del aquél y se encuentre debidamente certificada o acreditada, tanto en lo que se refiere a su independencia como en lo que atañe a sus procedimientos de actuación, y se permita, en todo caso, al cliente manifestar su opinión y como acceder a los resultados del informe de auditoría que deberá reunir los requisitos a que hace referencia el Dictamen 5/2012 al que se viene haciendo referencia.

III

En cuanto a si la segunda cláusula transcrita en la consulta cumple los requisitos del 21 del Reglamento de desarrollo de la Ley Orgánica 15/1999, debe recordarse que una de las especificaciones que debe contener el contrato es la de la prohibición al proveedor de comunicar los datos a terceros, ni siquiera para su conservación, salvo que se prevea la existencia de subcontratistas.

El artículo 21 del Reglamento de desarrollo de la Ley Orgánica 15/1999, dispone que *“1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.*

2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:



a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior.”

De este modo, el responsable (en el presente caso el consultante) debe conocer quienes serán los subcontratistas toda vez que los contratos que firme el encargado con ellos se efectuarán en nombre y por cuenta del responsable. A su vez, el encargado debe firmar con el subcontratista un contrato en el que éste garantice el cumplimiento de las instrucciones del responsable del fichero.

En este sentido, el Grupo de Trabajo del artículo 29 en el Dictamen al que se viene haciendo referencia pone de manifiesto la necesidad de garantizar la transparencia en la relación entre el cliente, el proveedor y los subcontratistas. Recuerda así que *“El cliente sólo es capaz de evaluar la legalidad del tratamiento de datos personales en la nube si el proveedor le informa sobre todas las cuestiones pertinentes”* y recomienda adoptar las siguientes salvaguardias relativas a la subcontratación: *“en los contratos entre proveedores y clientes deberán preverse disposiciones relativas a los subcontratistas. Los contratos deberán especificar que sólo podrá contratarse a subencargados del tratamiento previa autorización general del responsable del tratamiento, en consonancia con la inequívoca obligación del encargado del tratamiento de informar al responsable de cualquier cambio previsto a este respecto, conservando el responsable del tratamiento en todo momento la posibilidad de oponerse a tales cambios o de rescindir el contrato. Debe existir una clara obligación para el proveedor de nombrar a todos los subcontratistas contratados. El proveedor deberá firmar un contrato con cada subcontratista que refleje las cláusulas de su contrato con el cliente; el cliente deberá asegurarse de que cuenta con posibilidades contractuales de recurso en caso de infracción del contrato por parte de los subcontratistas del proveedor.”*



Por otra parte, debe tenerse en cuenta que, como consecuencia del encargo del tratamiento o de las sucesivas subcontrataciones, puede originarse una transferencia internacional de datos, el artículo 5.1 s) del Reglamento de desarrollo de la Ley Orgánica 15/1999, define estas como el *“tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español”*.

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

De este modo la transmisión de datos a entidades situadas fuera del Espacio Económico Europeo constituirá una transferencia internacional de datos que deberá respetar el régimen establecido en los artículos 33 y 34 de la Ley Orgánica 15/1999 y en el Título VI de su Reglamento de desarrollo.

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

El artículo 33.2 de la Ley Orgánica 15/1999 establece los criterios para determinar el carácter adecuado de protección al disponer que *“el carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos de finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países”*. En este sentido cabe recordar que la Comisión de la Unión Europea ha adoptado decisiones en las que se ha considerado que existe un nivel adecuado de protección en Estados tales como Suiza, Argentina, Uruguay, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Canadá respecto de las entidades sujetas



al ámbito de aplicación de la ley canadiense de protección de datos y las entidades estadounidenses adheridas a los «principios de Puerto Seguro».

De este modo el consultante, debe conocer la cadena de subcontrataciones a fin de estar informado donde pueden localizarse los datos y si el país tiene un régimen de garantías adecuado, debiendo solicitar la correspondiente autorización de la Agencia en caso contrario. Señala en este sentido el Dictamen 5/2012 que la transparencia en la nube supone que es necesario que el cliente tenga conocimiento de todos los subcontratistas que contribuyan a la prestación de los respectivos servicios en nube, así como de la localización de todos los centros donde puedan tratarse los datos personales. Sólo entonces podrá evaluar si los datos personales pueden ser transferidos a un llamado tercer país fuera del Espacio Económico Europeo (EEE) que no garantice un nivel adecuado de protección en el sentido de la Directiva 95/46/CE.

Igualmente esta Agencia ha señalado en el aludido informe de 2012 que debe existir un procedimiento que permita al responsable acceder a los datos de identificación de los contratistas y, en el caso de transferencias internacionales o de subcontrataciones posteriores a la transferencia, la ubicación geográfica en que se prestará el servicio, procedimiento que podrá consistir en el acceso a través de una página web, a la que se haga expresa referencia en el contrato, a los datos de identificación de los subcontratistas, ubicación de los mismos y servicios de tratamiento que éstos van a desarrollar.

En lo que respecta a las posibles transferencias internacionales de datos resulta de especial interés lo señalado por el Grupo de Trabajo del artículo 29 en el Dictamen 5/2012 respecto a los principios de Puerto Seguro al señalar que “Las transferencias a organizaciones de estadounidenses que están adheridas a los principios pueden realizarse legítimamente en virtud de la legislación de la UE, ya que se considera que las organizaciones beneficiarias proporcionan un nivel adecuado de protección de los datos transferidos.

El Grupo de Trabajo del artículo 29 recuerda que el artículo 17 de la Directiva de la UE requiere la firma de un contrato entre el responsable y el encargado del tratamiento a efectos del tratamiento de datos, lo que se confirma en la FAQ 10 de la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, sobre la adecuación de la protección conferida por los principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América. Este contrato no está sujeto a la autorización previa de las autoridades de protección de datos europeas. Dicho contrato especifica el tratamiento que debe efectuarse y las medidas necesarias para garantizar que los datos están seguros. (...).

Ahora bien, el Grupo de Trabajo del artículo 29 considera que las empresas exportadoras de datos no deben basarse únicamente en la declaración del importador de datos de que tiene una certificación de Puerto Seguro. Por el contrario, la empresa que exporta datos debe obtener pruebas de la existencia de

las autocertificaciones de Puerto Seguro y solicitar pruebas de que se cumplen sus principios.(...)

El Grupo de Trabajo del artículo 29 también considera que el cliente debe comprobar si los contratos tipo elaborados por los proveedores cumplen los requisitos nacionales sobre tratamiento de datos contractual. La legislación nacional puede exigir que el subtratamiento se defina en el contrato, lo que incluye datos sobre los lugares y otros relativos a los subencargados del tratamiento, así como la trazabilidad de los datos. Normalmente, los proveedores no ofrecen al cliente tal información, su compromiso con el Puerto Seguro no puede sustituir la falta de las garantías anteriormente mencionadas, cuando así lo exija la legislación nacional. (...)

Por último, el Grupo de Trabajo del artículo 29 señala que, en términos de seguridad de los datos, la computación en nube plantea varios riesgos de seguridad específicos de la nube, tales como pérdida de gobernanza, supresión de datos insegura o incompleta, pistas de auditoría insuficientes o fallos de aislamiento, que no son tenidos suficientemente en cuenta por los actuales principios de Puerto Seguro sobre la seguridad de los datos. Así pues, podrán establecerse garantías adicionales para la seguridad de los datos, por ejemplo mediante la incorporación de conocimientos y recursos de terceros que sean capaces de evaluar la adecuación de los proveedores mediante distintos sistemas de auditoría, normalización y certificación. Por estos motivos, podría ser aconsejable complementar el compromiso del importador de datos con el Puerto Seguro con salvaguardias adicionales que tengan en cuenta la naturaleza específica de la nube.

De todo ello se desprende que la cláusula aportada por el consultante no da cumplimiento a lo previsto en el artículo 21 de la Ley Orgánica 15/1999, debiendo, además, tener presente al contratar el servicio objeto de consulta los aspectos relativos 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 Puerto Seguro para la prestación de dichos servicios de cloud computing, tal y como viene a señalar el Grupo de Trabajo del artículo 29.

Las dificultades que plantean a los responsables del fichero o tratamiento la necesidad de recabar en cada caso la autorización del director de esta Agencia para la transferencia internacional de datos y las comprobaciones a que hace referencia el Grupo de Trabajo del artículo 29 respecto de la adhesión a los principios de Puerto Seguro de los subcontratistas, podrían ser obviadas, como señalaba el citado informe de 2012 de esta Agencia, en el supuesto de que por el prestador del servicio de cloud computing se adoptasen unas cláusulas estandarizadas que, conteniendo las garantías adecuadas de protección de los derechos de los afectados, y en particular de su derecho fundamental a la protección de datos, fuesen aprobadas por esta Agencia. Existiría así una autorización automática de cualquier transferencia internacional realizada al amparo de tales cláusulas en tanto no se produjera ninguna alteración de las mismas, de modo que el cliente (esto es,



el responsable del fichero) únicamente tendría que notificar la modificación del fichero cuyos datos fueran objeto de transferencia como consecuencia de la contratación del servicio de computación en nube.