N/REF: 166517/2016

Se solicita un informe en el que se evalúe si la solución de mensajería electrónica denominado “MICROSOFT OFFICE 365 EXCHANGE” cuenta con la aprobación de la Agencia Española de Protección de Datos en cuanto al cumplimiento de la normativa europea y española vigente en materia de Protección de Datos, al estar valorándose por la Administración Pública consultante la posibilidad de adoptar como solución de mensajería electrónica el citado sistema.

Como carácter previo debe señalarse que entre las competencias de esta Agencia no figura la de emisión de aprobaciones en cuanto al cumplimiento de la normativa de protección de datos de ningún tipo de servicio prestado por entidades públicas o privadas, sin perjuicio de que determinados tratamientos, como los movimientos internacionales de datos, puedan exigir una autorización en los casos expresamente previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. No obstante, esta Agencia viene atendiendo, en la medida de lo posible, 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 antes de realizar actuaciones que pudieran, eventualmente, considerarse contrarias al Derecho, evitando así incumplimientos involuntarios de la legislación vigente.

En el marco de esta actividad de asesoramiento, cabe hacer referencia a determinadas cuestiones que el solicitante debe examinar a fin de comprobar si su actuación resulta conforme a lo establecido en la normativa de protección de datos. Tratándose en el presente supuesto de la contratación de un servicio de Cloud Computing, cabe señalar que esta Agencia ha publicado un guía, disponible en su página web http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf, en la que se analizan los riesgos que puede plantear la adopción de esta solución tecnológica, las garantías y compromisos exigibles entre otras cuestiones y se realiza una particular referencia a la contratación de este tipo de servicios por las Administraciones Públicas.

Como punto de partida debe señalarse que el responsable del fichero o tratamiento, en este caso la Administración consultante, que contrata un servicio de cloud computing debe tener en cuenta que su responsabilidad no se desplaza al proveedor del servicio aunque sea una gran compañía multinacional o incorpore una cláusula al respecto, por lo que deberá analizar los riesgos que genera dicho servicio para determinar si traslada información al mismo y, en su caso, qué clase de información.

En lo que respecta a los riesgos a que desde el punto de vista de la normativa de protección de datos puede dar lugar la utilización de un servicio de cloud computing, cabe hacer una referencia a 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. En dicho Dictamen se analizan 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 Espacio Económico Europeo. 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 guía publicada por esta Agencia para quienes contratan un servicio de cloud computing a la que anteriormente se hacía referencia señala específicamente en lo que respecta a las Administraciones públicas lo siguiente:

"El volumen y la sensibilidad de los datos que gestionan las Administraciones Públicas conllevan unos riesgos específicos que deben

ser objeto de un análisis riguroso en cada escenario en el que se plantee su utilización. Estos riesgos específicos aconsejan la adopción de cautelas adicionales en su implantación, de forma que no se vean comprometidos los derechos y la seguridad de los ciudadanos.

La posibilidad de tratamiento de los datos fuera del territorio nacional, característica del *cloud computing*, constituye un elemento de especial relevancia en el caso de las Administraciones Públicas. En este sentido, debe tenerse en cuenta que la normativa que regula los movimientos internacionales de datos es aplicable tanto a entidades públicas como privadas.

En particular, debe tenerse muy presente que Autoridades competentes de terceros países en los que se traten datos personales en el marco de los servicios de *cloud computing* podrían solicitar y acceder a la información de la que las Administraciones públicas son responsables, en algunos casos, sin que se le informe de esta circunstancia. Por ello es fundamental obtener información del prestador de servicios de *cloud computing* sobre si existe esta posibilidad en alguno de los países donde se vayan a tratar los datos, si la Administración contratante puede conocer o no tales requerimientos, así como las decisiones que puede tomar al respecto. La trascendencia de estos posibles accesos es un factor muy relevante para decidir sobre la contratación de estos servicios y el proveedor que los vaya a prestar."

Así pues, la Administración Pública consultante, debe analizar los riesgos que puede presentar el servicio de cloud computing que pretende contratar y la información que pretenda almacenar en la nube. Si efectuado dicho análisis determina la contratación de tal servicio, deberá tener en cuenta los requerimientos que a continuación se examinan.

I

En primer término, debe tenerse en cuenta, que la normativa de protección de datos aplicable será la del país en que esté establecido el responsable del fichero o tratamiento que contrata los servicios de computación en nube y no la del lugar en que se encuentren los proveedores de dichos servicios, resultando así de aplicación al presente supuesto en que el responsable es una Administración pública española la normativa de protección de datos vigente en España.

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. Dicha guía recuerda 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.

Conforme a dicha normativa, la inclusión de datos personales en servicios de computación en nube exige la existencia de 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.

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.

Debe aquí pues hacerse expresa referencia a los requisitos que el artículo 12 de la Ley Orgánica 15/1999 exige para que la relación entre responsable y encargado de tratamiento pueda considerarse como tal:

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".*

En segundo lugar, 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".*

En cuanto a las medidas de seguridad que hayan de ser adoptadas por quienes realicen trabajos de tratamiento de datos por cuenta de tercero, deberán ser estipuladas en el contrato tal y como dispone el último párrafo del artículo 12.2 de la Ley Orgánica 15/1999.

Asimismo, debe hacerse una especial referencia a la subcontratación, ya que 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. Cabe así recordar 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."

Por su parte, la disposición adicional vigésima sexta 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, regula la subcontratación de servicios por parte del encargado del tratamiento, exigiendo lo siguientes tres 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.

De este modo, el responsable (en el presente caso el consultante) debe conocer quiénes 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."

Cabe aquí reseñar que esta Agencia emitió informe con fecha 25 de julio de 2012, en el que se analizaba la posibilidad de que un proveedor de servicios firmase un único contrato con cada subcontratista, que cubriese todas las actividades de tratamiento que el mismo fuese a llevar respecto de los datos de todos los clientes, considerando que dicha solución podría considerarse que aporta garantías suficientes siempre que el cliente del servicio de computación en nube pueda tener claro conocimiento de la identidad de los terceros subcontratistas del servicio, así como de las actividades desplegadas por cada uno de ellos.

Señalaba el aludido informe de 25 de julio de 2012 que ello debería acompañarse de un procedimiento que permitiera a los clientes acceder a los citados datos de identificación y, en el caso de transferencias internacionales de datos, la ubicación geográfica en que se prestará el servicio. Consideraba dicho informe que sería suficiente a efectos de acreditar la existencia de garantías adecuadas que los clientes pudieran acceder, por ejemplo, a través de un sitio web al que se hiciera expresa referencia en el contrato firmado con la consultante, a los datos de identificación de los subcontratistas, ubicación de los mismos y servicios de tratamiento que aquéllos desarrollarán, bastando la celebración de un contrato único con tales subcontratistas siempre que, lógicamente, cumpliese con los requisitos necesarios para que cupiera atribuir a los mismos la condición de subencargados del tratamiento o para adoptar garantías suficientes en caso de transferencia ulterior de los datos.

Por consiguiente el consultante deberá firmar con el proveedor del servicio de cloud computing el acuerdo al que se refiere el artículo 12 de la Ley Orgánica 15/1999, debiendo igualmente autorizarse la subcontratación de los servicios en los términos establecidos en la disposición adicional vigésima sexta del Real Decreto Legislativo 3/2011, debiendo tener conocimiento de la identificación de los subcontratistas, los servicios que éstos prestan y su ubicación, tanto en el momento de la firma del contrato como durante su vigencia a fin de poder revocar en su caso el contrato cuando no esté conforme con los posibles cambios de los subcontratistas.

II

Debe tenerse en cuenta también, que, como consecuencia del encargo del tratamiento o de las sucesivas subcontrataciones, puede originarse una transferencia internacional de datos, definida en el artículo 5.1 s) del Reglamento de desarrollo de la Ley Orgánica 15/1999 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 emitido por el Grupo de Trabajo del artículo 29, según el cual "*la computación en nube se basa a menudo en la total falta de ubicación estable de los datos en la red del proveedor. Los datos pueden encontrarse en un centro de datos a las 2 horas y en el otro lado del mundo a las 16 horas. Por tanto el cliente rara vez se encuentra en posición de saber en cualquier momento en qué lugar están situados, almacenados o transferidos los datos."*

La transmisión de datos a entidades situadas fuera del Espacio Económico Europeo 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 y Canadá respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos.

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. 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, 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 consecuencia, el responsable del tratamiento debe conocer la cadena de subcontrataciones a fin de estar informado de dónde 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.

Como ya se ha indicado, 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.

No obstante, en lo que al presente supuesto respecta se aporta una Resolución de esta Agencia de 9 de mayo de 2014, recaída en el expediente de autorización de transferencias internacionales de datos con referencia TI/32/2014 en la que se acordaba expresamente lo siguiente:

"Primero.- Considerar adecuadas las garantías establecidas en los modelos de contratos aportados por MICROSOFT CORPORATION para la transferencia internacional de datos con destino a dicha entidad, establecida en los Estados Unidos, con motivo de la prestación de los servicios OFFICE 365, MICROSOFT DYNAMICS CRM ONLINE y WINDOWS AZURE (MOS) y actuando como encargado del tratamiento.

Segundo.- Considerar autorizadas las transferencias internacionales de datos con destino a los Estados Unidos que se realicen al amparo de las cláusulas contractuales mencionadas, siempre que se cumplan las siguientes condiciones:

1. La finalidad de la transferencia será la prestación de los servicios OFFICE 365, MICROSOFT DYNAMICS CRM ONLINE y WINDOWS AZURE (MOS) por parte de MICROSOFT CORPORATION, actuando como encargado del tratamiento. Los datos se transfieren en las condiciones y con todas las garantías reseñadas en los Fundamentos de Derecho anteriores.

2. La autorización sólo podrá entenderse concedida en caso de que el contrato firmado entre los responsables exportadores de los datos y MICROSOFT CORPORATION incorpore la totalidad de los documentos que se han aportado para la adopción de la presente resolución para cada uno de los servicios a los que la misma se refiere.

3. El exportador de datos deberá notificar al RGPD los ficheros cuyos datos vayan a ser objeto de transferencia internacional con carácter previo, con indicación de su denominación y código de inscripción en el RGPD, indicando que se producirá la transferencia internacional de los datos al amparo de la presente resolución.

4. El alcance de la transferencia internacional de datos que se lleve a cabo deberá resultar ajustado a la estructura del fichero, categorías de datos y finalidades del tratamiento establecidas en la inscripción del correspondiente fichero.

5. El exportador de datos deberá poner a disposición de la AEPD, cuando le fueran requeridos, los contratos de prestación de servicios que haya suscrito con MICROSOFT IRELAND OPERATIONS LIMITED (MIOL) y MICROSOFT CORPORATION (…).”

Por consiguiente, esta Agencia ya ha considerado que las transferencias internacionales de datos que pudieran llevarse a cabo mediante la contratación de los servicios mencionados en la resolución parcialmente transcrita reúnen garantías suficientes que permiten su autorización, sin que sea preciso para el responsable, en este caso el consultante, obtener una autorización específica para llevar a cabo dichas transferencias. No obstante, deberá notificar al Registro General de Protección de Datos que se van a llevar a cabo transferencias internacionales de datos a fin de que se modifique la inscripción del fichero, en la forma prevista en los artículos 52 y siguientes del Reglamento de desarrollo de la Ley Orgánica 15/1999.

III

En lo que respecta a las medidas de seguridad a aplicar, el artículo 9.1 de la Ley Orgánica 15/1999 impone al responsable del fichero, esto es el consultante, y, en su caso, al encargado la obligación de adoptar las medidas técnicas y de organización que garanticen la seguridad de los datos de carácter personal. Debe aquí recordarse que el artículo 12.2 de la misma Ley exige que dichas medidas de seguridad se estipulen en el contrato entre responsable y encargado de tratamiento.

El número tercero del artículo 9 de la citada Ley señala que “*Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.”*

El Reglamento de desarrollo de la Ley Orgánica 15/1999, constituye en la actualidad la normativa vigente en materia de medidas de seguridad aplicables a los tratamientos de datos de carácter personal. El artículo 80 de esta norma clasifica las medidas de seguridad aplicables a los ficheros o tratamientos de datos en tres niveles, debiendo adoptarse, en cada caso, el nivel correspondiente en función de la naturaleza de los datos a tratar.

Asimismo, en el presente caso resulta de aplicación la normativa vigente en materia de Administración electrónica, en particular, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Debe tenerse en cuenta que el Esquema nacional de seguridad se aplica en un ámbito más amplio que la normativa de protección de datos, en tanto debe implementarse con independencia de que se traten o no datos personales, y su objetivo viene determinado en el artículo 2.1 del Real Decreto 3/2010 citado según el cual "*El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.*

Por su parte, la normativa de protección de datos sólo es exigible cuando se tratan datos de carácter personal, si bien en la mayor parte de los supuestos la información administrativa a la que debe aplicarse el Esquema Nacional de Seguridad contendrá datos de carácter personal. Debe tenerse en cuenta que, a diferencia de esta última norma, para determinar el nivel de medidas de seguridad a adoptar conforme al Reglamento de desarrollo de la Ley Orgánica 15/1999 debe estarse a la naturaleza de los datos objeto de tratamiento.

De este modo, ambas normativas concurren en el caso que nos ocupa, teniendo las dos el carácter de mínimos exigibles, cuya implantación viene impuesta imperativamente por el ordenamiento jurídico, por lo que resulta preciso dar cumplimiento a los requisitos que cada una de ellas establece. Dispone a estos efectos el artículo 27 del esquema de seguridad que:

"*1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las Administraciones públicas aplicarán las medidas de seguridad indicadas en el Anexo II, teniendo en cuenta:*

a) Los activos que constituyen el sistema.

b) La categoría del sistema, según lo previsto en el artículo 43.

c) Las decisiones que se adopten para gestionar los riesgos identificados.

2. Cuando un sistema al que afecte el presente real decreto maneje datos de carácter personal le será de aplicación lo dispuesto en la Ley Orgánica

15/1999, de 13 de diciembre, y normativa de desarrollo, sin perjuicio de los requisitos establecidos en el Esquema Nacional de Seguridad.

3. Los medidas a las que se refieren los apartados 1 y 2 tendrán la condición de mínimos exigibles, y podrán ser ampliados por causa de la concurrencia indicada o del prudente arbitrio del responsable de la información, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos."

Debe señalarse que una buena parte de las medidas de seguridad que el Reglamento de desarrollo de la Ley Orgánica 15/1999 establece para ficheros o tratamientos automatizados son coincidentes con las establecidas en el Esquema Nacional de Seguridad; no obstante en algunos casos no existe plena concordancia en los requerimientos técnicos exigibles en uno y otro caso. Cabe así destacar las medidas relativas al registro de incidencias (artículos 90 y 100 del aludido Reglamento) y al registro de accesos (artículo 103 de la misma norma). En aquellos supuestos en que los requerimientos técnicos sean diferentes, será preciso dar cumplimiento a los requisitos exigidos por cada normativa.

La guía para clientes que contraten servicios de cloud computing a la que se ha hecho referencia señala a este respecto que la implantación de tales servicios incide de forma singular en algunos elementos del Esquema Nacional de Seguridad, mencionando entre otros aspectos la protección de la información almacenada y en tránsito mediante medidas de cifrado para garantizar su confidencialidad, la realización de copias de respaldo y la adecuada gestión de las incidencias de seguridad y mecanismos que garanticen la continuidad de las operaciones en caso de catástrofes o incidentes severos.

En el presente supuesto, dado que se aporta un certificado de conformidad con el esquema nacional de seguridad, deberá examinarse qué medidas de seguridad, teniendo en cuenta la naturaleza de los datos objeto de tratamiento, exige el Reglamento de desarrollo de la Ley Orgánica 15/1999, y en caso de que deban adoptarse medidas de seguridad que no estuviesen contenidas en el Esquema nacional de Seguridad, implementar las mismas.

Entre otras, cabe mencionar que debe hacerse constar en el documento de seguridad la prestación de servicios de cloud computing por encargados de tratamiento, conforme a lo señalado en el artículo 88 de dicho Reglamento. Igualmente, el acceso a la información debe reunir un nivel de medidas de seguridad equivalente al de los accesos en modo local, tal y como dispone el artículo 85 del Reglamento de desarrollo de la Ley Orgánica 15/1999. En el supuesto de que, por tratarse de datos que exijan medidas de seguridad de nivel medio o alto, deba realizarse la auditoría a que se refiere el artículo 96 del Reglamento, la misma debe venir referida al cumplimiento de las medidas de seguridad a que se refiere dicha norma, con independencia de que pueda

hacerse conjuntamente con otra que verifique el cumplimiento de los requerimientos del Esquema Nacional de Seguridad.

Por último, cabe mencionar en particular, la necesidad de incluir entre las medidas de seguridad la obligación del proveedor del servicio de informar al consultante cuando se produce una incidencia de seguridad que afecte a los datos personales de que éste es responsable, de las medidas adoptadas por el encargado para resolver tal incidencia y, en su caso, de las medidas que el responsable debe adoptar para evitar daños a los titulares de los datos personales. Dicho deber, aunque no esté recogido expresamente en el Reglamento, puede derivarse entre otros preceptos, del artículo 20.2 del Reglamento que introduce un poder de supervisión del responsable sobre el encargado, que le legitima para verificar el cumplimiento de las medidas de seguridad antes y durante la vigencia del contrato y adoptar las medidas correctoras oportunas.

IV

Por último, cabe hacer referencia a otras cuestiones a las que igualmente se refiere la aludida guía de contratación en cloud computing, que es conveniente incorporar, si no lo estuviesen, al contrato a celebrar con el proveedor del servicio.

Cabe destacar en primer lugar el aspecto relativo a la portabilidad de los datos, ya que incide particularmente en la obligación del proveedor del servicio de devolver los datos al responsable al finalizar la prestación del mismo o a un nuevo encargado del tratamiento designado por el responsable, tal y como prevé el Reglamento de desarrollo de la Ley Orgánica 15/1999 en su artículo 20.3.

Como se señalaba al principio de este informe, uno de los riesgos que plantea el servicio de cloud computing puede ser la falta de disponibilidad de los datos si el formato utilizado por el proveedor no resulta interoperable. Así el consultante, deberá comprobar y exigir en su caso, que a la finalización del servicio se le entreguen los datos en el formato que se acuerde, que cumpla los requisitos establecidos en el Esquema Nacional de Interoperabilidad, a fin de poder almacenarla en sus propios sistemas o permitir su traslado a un nuevo proveedor que el responsable contrate con total garantía de la integridad de la información.

Señala en este sentido la guía a que venimos haciendo referencia que “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"

También resulta de interés incluir una cláusula que garantice que el proveedor no conservará los datos personales una vez extinguido el contrato. La guía hace referencia a mecanismos como la certificación de destrucción emitida por el propio proveedor o un tercero. Cabe aquí recordar que el artículo 22.2 del Reglamento de desarrollo dela Ley Orgánica 15/1999 faculta al encargado del tratamiento a mantener los datos bloqueados en tanto puedan derivarse responsabilidades de su relación con el responsable. Ahora bien, una vez finalizado el plazo de garantía contractual deberá procederse por el encargado del tratamiento al borrado de los datos.