AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

RESOLUCIÓN DE DECLARACIÓN DE ADECUACIÓN DE GARANTÍAS PARA LAS TRANSFERENCIAS INTERNACIONALES DE DATOS A LOS ESTADOS UNIDOS CON MOTIVO DE LA PRESTACIÓN DE SERVICIOS DE COMPUTACIÓN EN NUBE

Nº Expediente: TI/00032/2014

Vista la solicitud formulada por D. A.A.A., en nombre y representación de la compañía MICROSOFT CORPORATION, y presentada ante esta Agencia Española de Protección de Datos (AEPD), y teniendo en cuenta los siguientes

A N T E C E D E N T E S D E H E C H O

Primero.- Con fecha 12 de febrero de 2014, la entidad MICROSOFT CORPORATION presentó un escrito en el que expone que presta los servicios de computación en nube (cloud computing) denominados: OFFICE 365, MICROSOFT DYNAMICS CRM ONLINE y WINDOWS AZURE (en adelante MOS: MICROSOFT ONLINE SERVICES) a través de MICROSOFT IRELAND OPERATIONS LIMITED (MIOL), establecida en Irlanda, que ofrece a los clientes la firma, junto con el correspondiente contrato comercial, de un acuerdo de tratamiento de datos.

Que los servicios MOS son prestados por MIOL por sí mismo o a través de subcontratistas, siendo Microsoft Corporation, sociedad matriz del Grupo Microsoft establecida en los Estados Unidos, el subcontratista principal que, a su vez, presta los servicios por sí misma o a través de subcontratistas que pueden estar situados fuera del Espacio Económico Europeo (EEE).

Que, con la finalidad de aportar las garantías suficientes para las transferencias de datos a MICROSOFT CORPORATION y a sus subcontratistas, ofrece a sus clientes la posibilidad de firmar las cláusulas contractuales tipo, adoptadas por la Comisión Europea en su Decisión 2010/87/UE, y un acuerdo suplementario a dichas cláusulas para adecuar a las características de los servicios de computación en nube la realización de las auditorías de las actividades de tratamiento y la subcontratación de operaciones de tratamiento con subencargados ulteriores del tratamiento.

Aporta un ejemplar de cada uno de los documentos que conforman el esquema de garantías contractuales y solicita que, al amparo de lo dispuesto en los artículos 33 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y 70.2 de su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RLOPD), por el Director de la AEPD se declare que las garantías establecidas en la documentación que presenta son adecuadas para realizar

transferencias de datos personales a los Estados Unidos y que los clientes que contraten los servicios MOS y suscriban los contratos aportados queden autorizados a realizarlas siempre y cuando las notifiquen previamente al Registro General de Protección de datos (RGPD).

Segundo.- La solicitud formulada por Microsoft Corporation incluye la siguiente documentación:

- Acreditación de la representación que ostenta la persona que actúa en nombre de Microsoft Corporation
- Acuerdo de tratamiento de datos para la contratación de los servicios Office 365 y Microsoft Dynamics CRM Online, a suscribir entre el cliente, responsable del tratamiento, y MIOL
- Acuerdo de tratamiento de datos para la contratación de los servicios Windows Azure, a suscribir entre el cliente, responsable del tratamiento, y MIOL
- Modelo de contrato que incluye las cláusulas contractuales tipo adoptadas por la Decisión de la Comisión Europea 2010/87/UE para la contratación de los servicios Office 365 y Microsoft Dynamics CRM Online, a suscribir entre el cliente, responsable del tratamiento exportador de datos, y Microsoft Corporation
- Modelo de contrato que incluye las cláusulas contractuales tipo adoptadas por la Decisión de la Comisión Europea 2010/87/UE para la contratación de los servicios Windows Azure, a suscribir entre el cliente, responsable del tratamiento exportador de datos, y Microsoft Corporation
- Acuerdo suplementario a las cláusulas contractuales tipo para la contratación de todos los servicios MOS, a suscribir entre el cliente, responsable del tratamiento exportador de datos, y Microsoft Corporation

Tercero.- Los detalles de las transferencias a las que se refiere la solicitud se especifican en el apéndice 1 de las cláusulas contractuales tipo y en el acuerdo suplementario, y se exponen a continuación:

a) Cláusulas contractuales tipo adoptadas por la Decisión de la Comisión Europea 2010/87/UE para la contratación de los servicios Office 365 y Microsoft Dynamics CRM Online y acuerdo suplementario:

   - El exportador será un cliente de los servicios online
   - El importador es Microsoft Corporation, compañía establecida en EEUU
   - Las categorías de interesados y de datos personales se entienden comprensivas de toda persona física identificada o identificable cuyos datos personales sean tratados por el cliente en los servicios online
   - Los datos personales a transferir incluyen datos especialmente protegidos, de cualquier sensibilidad
   - Los datos personales transferidos serán sometidos a las siguientes operaciones básicas de tratamiento: los datos del cliente serán objeto de las operaciones de tratamiento asociadas a los servicios online contratados, incluyendo, entre otras, el almacenamiento, acceso y su transmisión.

b) Cláusulas contractuales tipo adoptadas por la Decisión de la Comisión Europea 2010/87/UE para la contratación de los servicios Windows Azure y acuerdo suplementario:

- El exportador será un cliente usuario de los servicios Core Platform
- El importador es Microsoft Corporation, compañía establecida en EEUU
- Las categorías de interesados y de datos personales se entienden comprensivas de toda persona física identificada o identificable cuyos datos personales sean tratados por el cliente en los servicios online
- Los datos personales a transferir incluyen datos especialmente protegidos, de cualquier sensibilidad
- Los datos personales transferidos serán sometidos a las siguientes operaciones básicas de tratamiento: los datos del cliente serán objeto de las operaciones de tratamiento asociadas a los servicios Core Platform contratados, incluyendo, entre otras, el almacenamiento, acceso y su transmisión.

F U N D A M E N T O S D E D E R E C H O

I

Es competente para dictar la presente resolución el Director de la Agencia Española de Protección de Datos conforme a lo dispuesto en el artículo 33 y 37.1.l) de la LOPD.

II

En la tramitación del presente procedimiento se han observado las normas previstas en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en los artículos 137 y siguientes del RLOPD.

III

El supuesto objeto de análisis en la presente resolución reviste ciertas especialidades respecto de los que han venido tradicionalmente siendo objeto de resoluciones de autorización de transferencias internacionales de datos. Ello se debe, en primer lugar, al hecho de que la documentación que ha de ser analizada ha sido presentada no por el exportador, sino por el importador de datos personales. Además, dicha documentación, formada por los correspondientes contratos relacionados con los servicios mencionados al comienzo de esta resolución, sus respectivos acuerdos suplementarios y adendas sobre el tratamiento de datos de carácter personal, se refiere a las garantías establecidas con carácter general en los supuestos de contratación de los servicios de computación en nube prestados por MIOL, sin hacer mención de un supuesto concreto de transferencia internacional de datos.

De este modo, el objeto de la presente resolución no puede ser la autorización de una concreta transferencia internacional, sino la determinación de si las garantías contenidas en la documentación aportada por Microsoft Corporation pueden considerarse adecuadas para permitir la realización de una transferencia internacional de datos en caso de que las mismas sean efectivamente cumplimentadas por los exportadores de datos que

pretendan la contratación con MIOL de los servicios de computación en nube a los que los contratos, siempre completados con su respectivos acuerdos suplementarios, se refieren.

A este respecto cabe señalar que el artículo 33.1 de la LOPD establece como norma general 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 Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas"* y el artículo 37.1.l) LOPD atribuye a la AEPD la función de *"ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos,…".*

De este modo, nada obsta a que por parte de esta Agencia pueda valorarse y resolverse si un determinado marco contractual, en el que se establezcan las distintas salvaguardas para que un cierto importador de datos de carácter personal proceda al tratamiento de aquéllos a los que el contrato se refiera, pueda incorporar garantías adecuadas a los efectos de permitir las futuras transferencias de datos que se lleven a cabo en el ámbito estricto de ese marco contractual.

Por este motivo, la presente resolución no podrá proceder automáticamente a la autorización de las transferencias internacionales de datos que fueran a llevarse a cabo, al no aparecer individualizada la entidad responsable que actuará en la transferencia como exportadora de los datos de carácter personal, pero sí podrá determinar si las transferencias que pudieran tener lugar conforme a las cláusulas sometidas al parecer de esta Agencia proporcionan las garantías suficientes para que una determinada transferencia internacional, realizada cumpliendo aquéllas, pueda considerarse merecedora de la correspondiente autorización, sin que para ello sea necesario recabar nuevamente el parecer de esta Agencia sino simplemente proceder a su notificación a la misma

IV

La entidad interesada manifiesta que es un prestador de servicios de computación en nube que ofrece a sus clientes la posibilidad de suscribir un conjunto de contratos para que, en los supuestos en los que se vayan a tratar datos de carácter personal, se aporten las garantías suficientes que permitan el flujo de datos a los Estados Unidos, país que no está declarado con un nivel de protección adecuado, y solicita que la Agencia Española de Protección de Datos considere que las transferencias internacionales de datos que como consecuencia de la contratación de los servicios MOS se realicen con destino a los Estados Unidos, utilizando el esquema de garantías que presenta, queden autorizados por proporcionar un nivel de protección suficiente.

La contratación de cualquier servicio MOS se realiza por el cliente, responsable del tratamiento, con Microsoft Ireland Operations Limited (MIOL), establecida en Irlanda, que actúa como encargado del tratamiento por lo que, junto al contrato comercial, ambas partes suscriben un acuerdo de tratamiento de datos. Aportan dos modelos de acuerdo, uno para los servicios Office 365 y Microsoft Dynamics CRM Online y otro para los

servicios de Windows Azure, en los que se contienen los extremos establecidos en el artículo 17 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 esos datos y en el 12 de la LOPD, así como la autorización del cliente para la subcontratación de los servicios prestados por MIOL y la posibilidad de que sean transferidos, así como conservados y tratados, a los Estados Unidos.

Así mismo, ofrecen al cliente la posibilidad de firmar con Microsoft Corporation, como importador de datos, las cláusulas contractuales tipo adoptadas por la Comisión Europea en su Decisión 2010/87/UE, que en su apéndice 1 establece los detalles de la transferencia de manera específica, por una parte, para los servicios Office 365 y Microsoft Dynamics CRM Online y, por otra, para los servicios de Windows Azure, y un acuerdo suplementario con la finalidad de adecuar a las características de los servicios de computación en nube la realización de las auditorías de las actividades de tratamiento cubiertas por las cláusulas y la subcontratación con subencargados ulteriores del tratamiento.

En este punto, debe tenerse en cuenta lo señalado por el Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE en su Dictamen 05/2012 sobre la computación en nube, adoptado el 1 de julio de 2012 (WP 196), en cuyo apartado 3.3.1 se señala lo siguiente:

"El cliente determina el objetivo último del tratamiento y decide sobre la externalización de este tratamiento y la delegación de la totalidad o de parte de las actividades de tratamiento a una organización externa. El cliente actúa por tanto como responsable del tratamiento. La Directiva define 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». El cliente, como responsable del tratamiento, debe aceptar la responsabilidad de respetar la legislación sobre protección de datos, y es responsable y está sujeto a todas las obligaciones legales que figuran en la Directiva 95/46/CE. El cliente podrá encargar al proveedor que elija los métodos y medidas técnicas y de organización adecuados para alcanzar los fines del responsable del tratamiento.

El proveedor es la entidad que presta los servicios de computación en nube de las distintas formas que se han mencionado. Cuando el proveedor suministra los medios y la plataforma, actuando en nombre del cliente, se considera que es el encargado del tratamiento es decir, con arreglo a la Directiva 95/46/CE, «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»."

Añade específicamente el Dictamen que *"el responsable del tratamiento debe elegir un proveedor que garantice el cumplimiento de la legislación sobre protección de datos. Debe prestarse una atención especial a las características de los contratos, que deberán incluir una serie de garantías de protección de datos normalizadas, incluidas las señaladas por el Grupo de Trabajo en el punto 3.4.3 (Medidas técnicas y de organización) y en el punto 3.5 (Flujos de datos transfronterizos), así como cualesquiera mecanismos adicionales que puedan resultar adecuados para facilitar la diligencia debida*

y la responsabilidad (como auditorías de terceros independientes y certificaciones de los servicios de un proveedor – véase el apartado 4.2)". Y concluye lo siguiente:

"Los proveedores (como encargados del tratamiento) tienen la obligación de garantizar la confidencialidad. La Directiva 95/46/CE establece que: «Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal». El acceso a los datos por parte del proveedor durante la prestación de servicios también se rige fundamentalmente por el requisito de cumplir las disposiciones del artículo 17 de la Directiva – véase el apartado 3.4.2.

Los encargados del tratamiento deben tener en cuenta el tipo de nube en cuestión (pública, privada, comunitaria o híbrida / IaaS, SaaS o PaaS [véase el anexo A) Modelos de implantación - b) Modelos de prestación de servicios]) y el tipo de servicio contratado por el cliente. Los encargados del tratamiento son responsables de la adopción de las normas de seguridad, de conformidad con las disposiciones de la legislación de la UE aplicadas en las jurisdicciones del responsable y del encargado del tratamiento. Los encargados del tratamiento deben también apoyar y asistir al responsable del tratamiento a respetar los derechos (ejercidos) de los interesados"

De este modo, la transferencia internacional que se plantea a partir de la documentación presentada debe reunir los requisitos necesarios para la transmisión transfronteriza de datos de un responsable del tratamiento (el exportador, cliente de los servicios) a un encargado del tratamiento (la entidad prestadora de los servicios de computación en nube). Por este motivo, se considera que la adopción, como base esencial de la transferencia, de las cláusulas contractuales contenidas en el Anexo de la Decisión 2010/87/UE puede considerarse adecuada.

V

El artículo 1 de la citada Decisión dispone que *"se considerará que las cláusulas contractuales tipo incluidas en el anexo ofrecen las garantías adecuadas con respecto a la protección de la vida privada y de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los correspondientes derechos, según exige el artículo 26, apartado 2 de la Directiva 95/46/CE".* Y el primer inciso del primer párrafo del artículo 2 añade que *"La presente Decisión aborda únicamente la adecuación de la protección otorgada por las cláusulas contractuales tipo establecidas en el anexo para la transferencia de datos personales a los encargados del tratamiento".*

La documentación aportada introduce, no obstante determinadas especialidades en el contenido de la relación contractual entre el cliente de los servicios y el importador de datos, referidas esencialmente a la realización de auditorías y a la posible subcontratación de servicios de computación en nube. Ello impide valorar de una forma directa si el conjunto del clausulado cumple efectivamente con las garantías exigidas por la citada Decisión, dado que una modificación en las cláusulas tipo no permite entender de una forma directa que las mismas se siguen ajustando a los estándares adoptados por la Comisión.

Así, por lo que respecta a las auditorías, la cláusula 5.f) de la Decisión 2010/87/UE estipula que el importador *"ofrecerá a petición del exportador de datos sus instalaciones de tratamiento de datos para que se lleve a cabo la auditoría de las actividades de tratamiento cubiertas por las cláusulas"* y que *"será realizada por el exportador de datos o por un organismo de inspección compuesto por miembros independientes con las cualificaciones profesionales necesarias y sujetos a la confidencialidad, seleccionado por el exportador de datos…"*. A su vez, la cláusula 12.2 determina que *"El importador de datos y el subencargado garantizan que, a petición del exportador o de la autoridad de control, pondrá a disposición sus instalaciones de tratamiento de datos para que se lleve a cabo la auditoría de las medidas mencionadas en el apartado 1* (relativas a las obligaciones una vez finalizada la prestación de los servicios de tratamiento de datos personales).

La segunda de las modificaciones de las cláusulas tipo de la Decisión 2010/87/UE afecta a lo estipulado en la cláusula 11, que dispone en su apartado 1 que *"El importador de datos no subcontratará ninguna de sus operaciones de procesamiento llevadas a cabo en nombre del exportador de datos con arreglo a las cláusulas sin previo consentimiento por escrito del exportador de datos. Si el importador de datos subcontrata sus obligaciones con arreglo a las cláusulas, con el consentimiento del exportador de datos, lo hará exclusivamente mediante un acuerdo escrito con el subencargado del tratamiento de datos, en el que se le impongan a este las mismas obligaciones impuestas al importador de datos con arreglo a las cláusulas. En los casos en que el subencargado del tratamiento de datos no pueda cumplir sus obligaciones de protección de los datos con arreglo a dicho acuerdo escrito, el importador de datos seguirá siendo plenamente responsable frente al exportador de datos del cumplimiento de las obligaciones del subencargado del tratamiento de datos con arreglo a dicho acuerdo". Por otra parte,* en el documento de preguntas más frecuentes relacionadas con las cláusulas 2010/87/UE, adoptado el 12 de julio de 2010 por el Grupo de Trabajo del artículo 29, se analiza el modo en que debe ser interpretada dicha previsión señalando que la firma de un único contrato para los supuestos de contratación no sería posible en el contexto de las cláusulas.

El acuerdo suplementario a las cláusulas contractuales tipo introduce determinadas estipulaciones que, como más adelante se expone, modifican sustancialmente el contenido de las cláusulas establecidas en el citado Anexo, lo que impide que se produzca de modo automático el efecto previsto en el artículo 1 de la citada Decisión, lo que exigirá proceder a su valoración, a fin de determinar si pueden ser consideradas como garantías suficientes a los efectos establecidos en el artículo 33.1 de la LOPD.

No obstante, es preciso tener en cuenta que las cláusulas referidas a "Definiciones", "Detalles de la transferencia", "Cláusula de tercero beneficiario", "Obligaciones del exportador de datos", "Obligaciones del importador de datos", salvo el apartado f) sobre la realización de auditorías que ha quedado modificado por el acuerdo suplementario, "Responsabilidad", "Mediación y Jurisdicción", "Cooperación con las autoridades de control", "Legislación aplicable", "Subtratamiento de datos", con la interpretación que se le da en el acuerdo suplementario, y la relativa a las "Obligaciones una vez finalizada la prestación de servicios de tratamiento de los datos personales", con la excepción de lo dispuesto en esta última cláusula sobre la realización de la auditoría, que igualmente se ha adecuado a las características de los servicios de computación en nube en el acuerdo suplementario a dichas cláusulas, son las mismas que las de la Decisión 2010/87/UE.

De este modo, y con las salvedades indicadas, que posteriormente se analizarán, los contratos vienen a incorporar en su mayor parte el clausulado de la citada Decisión, por lo que ha de considerase que proporcionan las garantías que han sido consideradas adecuadas por dicha Decisión.

VI

Como ya se ha indicado, y una vez se ha puesto de manifiesto que la mayor parte del clausulado aportado reproduce lo establecido en la Decisión 2010/87/UE, es preciso valorar a continuación si aquellos aspectos en los que las cláusulas se apartan de la literalidad del Anexo de dicha Decisión las garantías aportadas permiten que puedan seguir siendo adecuadas para que proceda autorizar las transferencias internacionales de datos basadas en las cláusulas que se están analizando.

El artículo 33.1 de la LOPD dispone 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*".

Por su parte, el artículo 70.1 del RLOPD dispone que "*Cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos"*.

En atención a lo anterior, el artículo 70.2 del RLOPD estipula que: *"La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito celebrado entre el exportador y el importador, 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".*

Exigencia de garantías suficientes cuyo origen se encuentra en el artículo 26.2 de la Directiva 95/46/CE, que dispone: *"…los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas."*

Se hace, por tanto, necesario valorar si las condiciones establecidas en los contratos presentados ofrecen esas garantías suficientes. Para ello hay que examinar si las estipulaciones del acuerdo suplementario a las cláusulas contractuales tipo de la Decisión 2010/87/UE, que las modifican en los dos aspectos señalados en el Fundamento de Derecho anterior, así como las incluidas en los acuerdos sobre el tratamiento de datos de

servicios MOS, que forman parte integrante del contrato, constituyen garantías suficientes.

VII

En lo que respecta a la potestad del cliente, exportador de datos, de realizar la auditoría de las actividades de tratamiento que implica la transferencia internacional de datos o de seleccionar el auditor, el punto 2 del acuerdo suplementario a las cláusulas contractuales tipo indica que "*el cliente acepta ejercitar su facultad de auditoría prevista en las cláusulas 5 (f) y 12 (2) de las Cláusulas Contractuales Tipo instruyendo a Microsoft Corporation a llevar a cabo la auditoría según lo descrito en el Acuerdo de Tratamiento de Datos y sin perjuicio del derecho a cambiar esta instrucción, según se reconoce en el mismo, cuyas disposiciones se entienden incorporadas al presente Acuerdo Suplementario mediante esta referencia*".

En el punto 4 b (ii) y 4 c (ii) de los acuerdos de tratamiento de datos para la contratación de los servicios Office 365 y Microsoft Dynamics CRM Online y Windows Azure, respectivamente (MOS) se indica que "*Microsoft auditará la seguridad de los ordenadores y el entorno de computación que utilice en el tratamiento de los Datos del Cliente (incluidos los datos personales) en los Servicios Online (Servicios Core Platform), así como los centros de datos físicos desde los que Microsoft presta los Servicios Online (todos los Servicios Windows Azure exceptuando Content Delivery Network). Esta auditoría: (a) se realizará al menos anualmente; (b) se ejecutará de acuerdo con los estándares ISO 27001; (c) será realizada por terceros profesionales en materia de seguridad, a elección y coste de Microsoft; (d) dará como resultado un informe de auditoría ("Informe de Auditoría Microsoft"), que constituirá información confidencial de Microsoft; y (e) podrá realizarse para otros fines adicionales al cumplimiento de esta cláusula (por ejemplo, como parte de los procedimientos habituales de Microsoft en materia de seguridad interna o para satisfacer otras obligaciones contractuales)*".

A la vista de esta información, debe valorarse si resulta posible interpretar que la facultad de los clientes de MOS de auditar las actividades de tratamiento se entendería colmada satisfactoriamente, si las partes acuerdan en las cláusulas, la posibilidad de que la auditoría se lleve a cabo mediante la contratación por la consultante de un tercero independiente, que goce de las adecuadas garantías de independencia de la importadora y acreditación de las labores de control llevadas a cabo por la misma.

Esta cuestión ha sido analizada por el Grupo de Trabajo del artículo 29 en el apartado 4.2 de su documento WP196 al indicar: "la realización de auditorías individuales de datos alojados en un medio de servidores virtualizados con múltiples operadores puede ser poco práctica desde el punto de vista técnico y puede en algunos casos aumentar los riesgos para los controles físicos y lógicos de seguridad de las redes. En tales casos, podrá considerarse que la auditoría por un tercero de reconocido prestigio elegido por el responsable del tratamiento puede sustituir el derecho de un responsable del tratamiento de realizar una auditoría.

De este modo, tomando en cuenta los criterios sustentados por el Grupo de Trabajo del artículo 29 en el citado Dictamen (WP196) sería posible considerar que la auditoría a la que se refieren los documentos contractuales aportados por Microsoft Corporation podría

ser considerada una garantía adecuada para la transferencia de datos derivada de la contratación de un servicio de computación en nube prestada por la misma (MOS).

Como se ha reproducido, el acuerdo suplementario a la cláusulas contractuales tipo y los dos acuerdos sobre tratamiento de datos en los servicios online (MOS) incorporan la posibilidad de que el cliente acepte que sea el importador quien audite, al menos anualmente, la seguridad de los ordenadores y el entorno de computación que utilice el tratamiento de los datos del cliente, llevándose a cabo la auditoría por terceros profesionales en materia de seguridad y concediéndose al cliente, si así lo solicita, el acceso a la información mediante un resumen confidencial del informe de auditoría llevada a cabo. Asimismo, se indica que si el cliente desea cambiar esta instrucción acerca del ejercicio de su facultad de auditoría tiene derecho a hacerlo según lo mencionado en las cláusulas contractuales tipo, solicitándolo por escrito.

Por ello, cabe considerar que estas condiciones proporcionan garantías suficientes para la transmisión de datos a los Estados Unidos en el marco de la prestación de servicios de computación en nube a los que se refiere el presente expediente.

VIII

La segunda de las modificaciones respecto a las cláusulas tipo contenidas en la Decisión 2010/87/UE se refiere a la subcontratación de la prestación de los servicios de tratamiento de datos, y se concreta en la posibilidad de llevar a cabo la firma de un único contrato con cada uno de los posibles subencargados del tratamiento, de modo que ese contrato cubra todos los tratamientos que éstos lleven a cabo respecto de los datos de los clientes del importador.

El apartado 3 del acuerdo suplementario a las cláusulas contractuales tipo señala a este respecto que “Microsoft Corporation podrá contratar a otras empresas para que presten servicios ilimitados en su nombre, tales como prestar servicios de soporte al Cliente. A cualquiera de estos subencargados únicamente se le permitirá obtener los Datos del Cliente para prestar los servicios que Microsoft Corporation le ha contratado que preste, y tendrá prohibido utilizar los Datos del Cliente con cualquier otra finalidad. Microsoft Corporation seguirá siendo responsable del cumplimiento de las obligaciones derivadas de las Cláusulas contractuales Tipo y del presente Acuerdo Suplementario por parte de sus subencargados. Todo subencargado al que Microsoft Corporation transfiera Datos del Cliente, incluso si es empleado con fines de conservación, habrá celebrado contratos por escrito con Microsoft Corporation que exijan que el subencargado cumpla unas condiciones no menos protectoras que las establecidas en las Cláusulas Contractuales Tipo y en el presente Acuerdo Suplementario; dichos contratos escritos también podrán ser de aplicación al tratamiento de datos de otros clientes. El Cliente ha consentido previamente que Microsoft Corporation transfiera los Datos del Cliente a los subencargados según lo descrito en las Cláusulas Contractuales Tipo y el presente Acuerdo Suplementario. Salvo por lo indicado más arriba o lo que el Cliente pueda autorizar de otro modo, Microsoft Corporation no transferirá a ningún tercero (ni siquiera con fines de conservación) datos personales que el Cliente proporcione a Microsoft Corporation a través del uso de los Servicios Online”.

A su vez, en el apartado 3 e) de los acuerdos sobre tratamiento de datos en servicios MOS se estipula que cada servicio MOS dispone de un sitio web que enumera los

subcontratistas que están autorizados a acceder a los datos del cliente y que, al menos 14 días antes de autorizar que un nuevo subcontratista acceda a los datos del cliente, Microsoft actualizará el correspondiente sitio web y proporcionará al cliente un mecanismo para obtener la notificación de dichas actualizaciones. Añade dicho apartado que si el cliente no aprobase a un nuevo subcontratista aquél podrá dar por terminado el servicio MOS afectado sin penalización alguna, remitiendo por escrito, antes de que finalice el periodo de notificación, una notificación de terminación que incluya una explicación de los motivos de la aprobación, y si el servicio online forma parte de una suite, o similar fórmula de contratación conjunta de varios servicios, la terminación se aplicará a la suite completa.

Como cuestión previa, el artículo 21 del RLOPD regula la subcontratación de servicios por un encargado del tratamiento, señalando lo siguiente:

"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".

Una previsión similar se contiene en el apartado 1 de la cláusula 11 del Anexo de la Decisión 2010/87/UE, que impone al importador la necesidad de haber obtenido la autorización por escrito del exportador para que la subcontratación ulterior pueda tener lugar.

Por otra parte, el Dictamen del Grupo de Trabajo del artículo 29 (WP196), al que ya se ha hecho referencia, señala, dentro de las directrices para los clientes y proveedores de servicios de computación en nube, lo siguiente:

"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 (véase el punto 3.3.2).”

Es decir, que si el cliente de los servicios MOS puede conocer la identidad de los subencargados y de las actividades que desplieguen no resultará un obstáculo el que la subcontratación se pueda acordar en un solo contrato con cada uno de los subcontratistas, siempre que el mismo especifique los servicios a prestar, y siempre que además se establezca un sistema que permita a los clientes conocer la identidad de los subencargados y su ubicación para el caso de transferencias ulteriores.

El acuerdo suplementario a las cláusulas contractuales incorpora la autorización del cliente para el uso de subencargados y, al propio tiempo, garantiza que los datos sólo se utilizarán para la prestación de los servicios subcontratados, con la prohibición de su utilización para cualquier otra finalidad, indicando expresamente que Microsoft Corporation es el responsable del cumplimiento de las cláusulas contractuales tipo y del acuerdo suplementario. Además, se añade expresamente que el subencargado habrá de firmar un contrato por escrito, que incluirá garantías no menos protectoras que las de las cláusulas tipo y el acuerdo suplementario.

Por otra parte, en los acuerdos sobre el tratamiento de datos, que forman parte de los contratos se estipula que cada servicio online dispone de un sitio web que enumera los subcontratistas que están autorizados a acceder a los datos del cliente. Al menos 14 días antes de autorizar que un nuevo subencargado acceda a los datos del cliente Microsoft actualizará el sitio web, y proporcionará una notificación a todos los clientes que se hayan suscrito a su recepción, y si el cliente no aprobase a un nuevo subcontratista podrá terminar el servicio online afectado sin penalización alguna remitiendo un escrito, antes de que finalice el periodo de notificación, explicando los motivos de la no aprobación.

Por todo ello, cabe considerar que las estipulaciones relativas a la subcontratación de los servicios de computación en nube que impliquen tratamiento de datos personales aportan garantías adecuadas para que el flujo de datos a los Estados Unidos pueda llevarse a cabo, conforme a lo establecido en el artículo 33.1 de la LOPD.

IX

Al propio tiempo, no puede ignorarse que tanto el acuerdo suplementario a las cláusulas contractuales tipo como los acuerdos sobre tratamiento de datos de los servicios MOS vienen a especificar con mayor precisión una serie de extremos que constituyen las garantías contenidas en la Decisión 2010/87/UE, especificando aún más las obligaciones del prestador de servicios. En particular, y además de las garantías establecidas en materia de auditoría de seguridad y subcontratación de los servicios, que al apartarse de la literalidad de la citada Decisión han exigido un estudio detallado en la presente resolución, deben tenerse particularmente en cuenta las condiciones estipuladas en los

acuerdos sobre el tratamiento de datos en los servicios online (MOS) en lo que respecta a la seguridad de los datos, incluidos en su apartado 4, así como la referencia a la notificación de incidentes de seguridad a la que se refiere el apartado 5 de dicho documento.

Además, el punto 6 del acuerdo suplementario añade que "El Cliente reconoce y acepta que, con independencia de que la exportación de datos personales aquí contemplada esté amparada por la Autorización AEPD, el Cliente tiene imperativamente, según la normativa española sobre protección de datos, la obligación propia de notificar a la AEPD la modificación de su inscripción del fichero o ficheros, mediante notificación en la que indique que procede a la exportación de datos personales a Microsoft Corporation al amparo de la Autorización AEPD. Esta notificación deberá especificar necesariamente, según la mencionada normativa, el fichero o ficheros del Cliente respecto de los que utilizará los Servicios Online".

Todo ello conduce a la conclusión de que las garantías aportadas en los contratos remitidos, siempre que los mismos incorporen tanto el acuerdo suplementario como las correspondientes adendas que han sido objeto de presentación ante esta Agencia Española de Protección de Datos, reúnen las garantías adecuadas exigidas por el artículo 33.1 de la LOPD para que quepa considerar susceptibles de autorización las transferencias internacionales de datos que pudieran llevarse a cabo como consecuencia de esos documentos.

X

La conclusión que acaba de alcanzarse conduce al necesario análisis de las consecuencias que pueden considerarse derivadas de esa declaración, toda vez que en el presente supuesto la valoración efectuada se lleva a cabo respecto del modelo contractual aportado y no en referencia a un supuesto concreto de transferencia internacional de datos de carácter personal.

Así, una vez consideradas adecuadas las garantías establecidas en el modelo contractual objeto de análisis en la presente resolución, la firma concreta del contrato por parte de un determinado cliente que pretenda la prestación de los servicios MOS a los que el modelo se refiere reuniría necesariamente las mismas garantías que se han valorado en la presente resolución.

De este modo, toda vez que el nivel adecuado de garantías ha sido suficientemente acreditado, la exigencia específica de una autorización individualizada de transferencia internacional de datos por cada uno de los clientes del servicio, siempre ajustada al artículo 33.1 de la LOPD en caso de reproducir ese marco contractual, ocasionaría una carga innecesaria al exportador solicitante, toda vez que la conclusión material del expediente resultaría prejuzgada por el contenido de esta resolución.

Por ello, establecido que las garantías aportadas son suficientes para llevar a cabo las transferencias internacionales de datos, parece razonable considerar que la declaración contenida en esta Resolución supone igualmente la autorización de las transferencias internacionales de datos que se lleven a cabo mediante la firma de las cláusulas contractuales analizadas, siempre que se observen una serie de requisitos:

- Las transferencias internacionales de datos deberán ajustarse a lo establecido en la presente resolución y en las cláusulas de los contratos presentados. Dichos contratos deberán incorporar el clausulado y la totalidad de los acuerdos suplementarios, anexos y adendas que han sido objeto de la presente resolución, dado que solamente en ese caso las garantías aportadas podrán considerarse suficientes con arreglo a la misma.

- El cliente, exportador de datos, deberá encontrarse en la situación de poder acreditar en todo momento ante esta Agencia que la transferencia se ha realizado con las garantías que aquí se han valorado, lo que exigirá la constancia documental de los contratos firmados con el prestador de servicio y con el importador de los datos.

- Con anterioridad a la realización de cualquier transferencia internacional de datos que pretenda ampararse en la presente resolución, el responsable del fichero deberá notificarla a la Agencia Española de Protección de Datos a fin de que se proceda a su inscripción en el Registro General de Protección de Datos, quedando identificados el fichero o ficheros a cuyos datos se refiera la transferencia internacional, con referencia a esta resolución.

- En todo caso, 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, cuyos datos vayan a ser objeto de transferencia para la prestación del servicio.

XI

Por último, debe recordarse que en todo caso, de conformidad con lo establecido en el artículo 70.3 del RLOPD, la transferencia o transferencias podrán denegarse o suspenderse temporalmente, con arreglo al procedimiento previsto en la sección segunda del capítulo V del Título IX del RLOPD, cuando concurra alguna de las circunstancias establecidas en el artículo 70.3 del citado Reglamento; es decir:

a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.
b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en las cláusulas contractuales aportadas.
c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.
d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.
e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

De manera que, no obstante la autorización concedida, la transferencia puede denegarse o suspenderse temporalmente si se diera alguna de estas circunstancias y sin perjuicio de las suspensiones que puedan acordarse de conformidad con lo estipulado en el contrato presentado.

En consecuencia, vistos los preceptos citados y demás de general aplicación, el Director

de la Agencia Española de Protección de Datos

RESUELVE

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.

6. La autorización de transferencia internacional podrá denegarse o suspenderse cuando concurra alguna de las circunstancias recogidas en el artículo 70.3 del RLOPD; es decir:

a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.
b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en las cláusulas contractuales aportadas.
c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.

d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.
e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

Tercero.- Ordenar que se dé traslado de la presente resolución al Registro General de Protección de Datos.

Cuarto.- Ordenar que se dé traslado de la presente resolución al Ministerio de Justicia, de conformidad con el artículo 139 del RLOPD, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995.

Quinto.- Ordenar que, de conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, la presente resolución se haga pública, una vez haya sido notificada a los interesados, en los términos previstos en artículo 116 del RLOPD.

Sexto.- Notificar la presente resolución al solicitante.

Contra esta Resolución, que pone fin a la vía administrativa, se podrá interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso-administrativo ante la Sala de lo Contencioso Administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, de conformidad con lo previsto en el artículo 46.1 del referido texto legal.

Madrid, 9 de mayo de 2014
EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

José Luis Rodríguez Álvarez