

Dictamen en relación a la consulta de una entidad de derecho público sobre la aportación de garantías adecuadas para la transferencia internacional de datos personales

Se presenta ante la Autoridad Catalana de Protección de Datos un escrito de una entidad de derecho público, en la que plantea si los instrumentos que se aportan incluyen garantías adecuadas para la transferencia internacional de datos personales a sus oficinas ubicadas en países respecto que no se ha declarado que ofrecen un nivel adecuado de protección.

Analizada la petición y visto el informe de la Asesoría Jurídica, se dictamina lo siguiente.

(...)

II

La entidad hace mención en su escrito al Dictamen CNS 6/2018 emitido en fecha 22 de febrero de 2018 por esta Autoridad en relación con una consulta formulada por esta misma entidad sobre la transferencia internacional de datos personales (en adelante, TID) a sus oficinas ubicadas fuera de Cataluña (disponible en la web <http://apdcat.gencat.cat>).

En este dictamen, la Autoridad analizó la TID que planteaba la entidad en atención a los países que serían destinatarios de la información personal, concluyendo, a los efectos que interesan en el presente dictamen, que:

“(...)

La transmisión de los datos a otros terceros países respecto a los cuales no se ha declarado que ofrecen un nivel adecuado de protección no podría efectuarse en el presente caso bajo la base legal de su necesidad por razones importantes de interés público (artículo 49.1 .d) RGPD), al no quedar suficientemente acreditado este extremo.

Tampoco podría efectuarse bajo la base legal de intereses legítimos imperiosos perseguidos por el responsable, excepción a que se refiere el párrafo segundo del artículo 49.1 del RGPD, al no resultar de aplicación a las actividades llevadas a cabo por autoridades públicas en el ejercicio de sus funciones (artículo 49.3 RGPD).

No obstante, salvo que pudiera resultar de aplicación alguna de las demás excepciones del artículo 49.1 del RGPD, la transmisión podría efectuarse si se aportan garantías adecuadas sobre la protección que los datos recibirán en su destino en los términos establecidos en el artículo 46 del RGPD. Esto, sin perjuicio del cumplimiento del resto de principios y obligaciones establecidos en materia de protección de datos.”

La entidad, a efectos de aportar las garantías a las que hace referencia este Dictamen CNS 6/2018, propone:

- a) Formalizar un contrato con las oficinas exteriores de la entidad que tienen personalidad jurídica propia, en el que se incorporen las cláusulas tipos de protección de datos adoptadas por la Comisión en la Decisión 2001/497/CE, de 15 de junio de 2001 .
- b) Formalizar un convenio con las oficinas exteriores de la entidad que carecen de personalidad jurídica propia, que incorpore cláusulas de similar naturaleza a las adoptadas por la Comisión en la Decisión 2001/497/CE, citada.

A continuación, plantea a esta Autoridad si estos instrumentos constituyen mecanismos adecuados para la realización de las TID, cuestión que se examina en los siguientes apartados de este dictamen.

III

Conviene recordar, de entrada, que la entidad, para poder ejercer las funciones que, por ley, le corresponden en materia de promoción empresarial, requiere que su personal desplazado a las oficinas de que dispone en terceros países (fuera de el Espacio Económico Europeo) pueda tener acceso remoto a las bases de datos de la entidad, constituyendo dicho acceso, tal y como se puso de manifiesto en el citado Dictamen CNS 6/2018 (FJ V), una TID.

Asimismo, recordar que las TID con destino a las oficinas de la entidad ubicadas en Ghana, Colombia, India, Marruecos, Turquía, Rusia, Chile, China, Corea del Sur, Emiratos Árabes, Sudáfrica, México, Brasil, Kenia, Singapur , Panamá, Perú, Australia, Estados Unidos (al estar fuera del Privacy Shield) y Canadá (no sometidas a Personal Information and Electronic Documents Act), dado que no consta que por ahora la Comisión haya adoptado una decisión sobre el nivel adecuado de protección que ofrecen estos países para los datos personales (artículo 45.3 RGPD), se podrán efectuar previa aportación de “garantías adecuadas ya condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas” (artículo 46.1 RGPD).

Señalar, en este punto, que de este listado de países (extraído del FJ VI del Dictamen CNS 6/2018) se ha excluido ahora a Japón, dado que recientemente la Comisión ha declarado que ofrece un nivel adecuado de protección (Decisión de 23 de enero de 2019). Por tanto, hay que tener en consideración que la TID hacia la oficina de la entidad ubicada en este país podría efectuarse sin necesidad de ninguna autorización específica, de conformidad con el artículo 45.1 del RGPD.

Tal y como se puso de manifiesto en el citado Dictamen CNS 6/2018 (FJ VI), el RGPD establece diferentes mecanismos para considerar que se ofrecen garantías adecuadas para transferir datos personales a un tercer país u organización internacional en los que no se garantiza un nivel de protección adecuado.

En concreto, el artículo 46.2 del RGPD dispone que:

“2. Las garantías adecuadas conforme al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:

- a) un instrumento jurídicamente vinculante y exigible entre las autoridades o organismos públicos; b) normas corporativas vinculantes de conformidad con el artículo 47; c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;

d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión conforme al procedimiento de examen a que se refiere en el artículo 93, apartado 2; e) un código de conducta aprobado conforme al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados, of) un mecanismo de certificación aprobado conforme al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.”

Y el artículo 46.3 del RGPD añade que:

“3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:

a) cláusulas contractuales entre el responsable o encargado y responsable, encargado o destinatario de las datos personales en el tercer país u organización internacional, ob) disposiciones que se incorporen en acuerdos administrativos entre las autoridades o organismos públicos que incluyan derechos efectivos y exigibles para los interesados.”

En relación con esta autorización de la autoridad de control competente, apuntar que la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDGDD), concreta, en el artículo 42, que “podrá otorgarse en los siguientes supuestos:

a) Cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con fundamento en cláusulas contractuales que no correspondan a las cláusulas tipo previstas en el artículo 46.2, letras c) y d), del Reglamento (UE) 2016/679. b) Cuando la transferencia se lleve a cabo por alguno de los responsables u encargados a los que se refiere el artículo 77.1 de esta ley orgánica y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades o organismos públicos de terceros Estados, que incorporan derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento.”

En atención a estas previsiones, parece desprenderse, a los efectos que interesan, que las autoridades u organismos públicos (recordar que la entidad tiene consideración de autoridad pública a efectos del RGPD (FJ VII del Dictamen CNS 6/2018)) disponen de mecanismos específicos a la hora de acreditar garantías adecuadas para la TID en terceros países, cuando su aportación sea necesaria.

Así, de acuerdo con el artículo 46.2.a) del RGPD, pueden utilizar “un instrumento jurídicamente vinculante y exigible”, tales como un acuerdo internacional bilateral o multilateral, o bien otro tipo de acuerdo administrativo que resulte vinculante y exigible para las partes sig

Esto parece que podría abarcar, al menos, los Tratados internacionales, los Acuerdos internacionales administrativos o los convenios firmados entre las administraciones públicas y los órganos, organismos públicos o entes de un sujeto de Derecho internacional sometidos al ordenamiento jurídico interno que determinen las partes (artículo 2.a) y b) de la Ley 25/2014, c

de noviembre, de tratados y otros acuerdos internacionales, y artículo 47.2 de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público).

Por otra parte, también pueden utilizar, de acuerdo con el artículo 46.3.b) del RGPD, acuerdos administrativos que, a pesar de legalmente no ser vinculantes para las partes, incluyan derechos efectivos y exigibles para los interesados. ”

Esto parece que podría abarcar aquellos acuerdos administrativos no normativos que contienen meras declaraciones de intenciones de contenido general o que establecen compromisos de actuación de carácter más bien político, técnico o logístico, siempre que no comporten la formalización de compromisos jurídicos concretos y exigibles, tales como los protocolos generales de actuación o los llamados memorandos de entendimiento, entre otros (artículo 2.c) Ley 25/2014 y artículo 47.1 Ley 40/2015).

Sin embargo, estos tipos de acuerdos deberían ser aprobados por esta Autoridad, a efectos de autorizar la TID (artículo 46.3 RGPD y artículo 42.1 LOPDGDD).

En cualquier caso, se opte por la vía del artículo 46.2.a) RGPD o por la del artículo 46.3.b) RGPD, hay que tener en consideración que lo importante es que los instrumentos incorporen garantías adecuadas sobre la protección que los datos transferidos recibirán en su destino (artículo 46.1 RGPD).

Precisamente por ello, no parece que debiera descartarse la posible utilización por parte de las autoridades y organismos públicos del resto de mecanismos o instrumentos a los que se refiere el artículo 46.2 y 3 del RGPD.

Éste podría ser el caso, por ejemplo, de acordar entre quien transferirá los datos (el exportador) y quien los recibirá (el importador) el uso de cláusulas de protección de datos, ya sean tipos (artículo 46.2.c) yd) RGPD) o ad hoc (artículo 46.3.a) RGPD).

De hecho, ésta parece ser la vía escogida en el presente caso por la entidad, a fin de acreditar garantías adecuadas para las TID en sus oficinas ubicadas en terceros países respecto a los cuales no se ha declarado un nivel de protección adecuado .

En concreto, la entidad, teniendo en cuenta la naturaleza jurídica de sus oficinas, propone dos mecanismos:

a) Por un lado, un contrato (del que no se adjunta copia) entre la entidad y sus oficinas exteriores que tienen personalidad jurídica propia, en el que se incorporen las cláusulas tipos de protección de datos adoptadas por la Comisión en la Decisión 2001/497/CE, de 15 de junio de 2001.

b) Por otro lado, un convenio (del que se adjunta copia) entre la entidad y sus oficinas exteriores que carecen de personalidad jurídica propia, que incorpore cláusulas de similar naturaleza a las adoptadas por la Comisión en la Decisión 2001/497 /CE.

Y, a efectos de formalizar este convenio, propone tres opciones:

Opción A. Firma del convenio por parte del responsable de la oficina exterior.

Opción B. Firma del convenio por parte del responsable de la oficina exterior así como por parte de todos los empleados y colaboradores de la oficina.

Opción C. Firma del convenio por parte del responsable de la oficina exterior y adhesión de el resto de empleados y colaboradores a través de sus contratos laborales.

También podría ser el caso, por ejemplo, de utilizar normas corporativas vinculantes (artículo 46.2.b) RGPD).

Estas normas son políticas de protección de datos a las que se adhiere un grupo empresarial para garantizar una adecuada protección de datos en las TID realizadas entre empresas de este grupo. Tienen que ser jurídicamente vinculantes y de obligado cumplimiento para todos los miembros que conforman el grupo empresarial o la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus trabajadores. Y, aparte de conferir expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, deben adecuarse a lo establecido en el artículo 47.2 del RGPD.

Ésta, cabe decir, podría ser otra opción a valorar en las TID a realizar por la entidad, teniendo en cuenta su naturaleza, funciones y, especialmente, funcionamiento (sede principal en Cataluña y una red de 40 oficinas exteriores repartidas en más de 100 países).

Por último, también podría plantearse utilizar códigos de conducta -aprobados de conformidad con el artículo 40 del RGPD- (artículo 46.2.e) RGPD) o mecanismos de certificación -aprobados de conformidad con el artículo 42 del RGPD - (artículo 46.2.f) RGPD).

Estos tipos de instrumentos pueden ofrecer garantías adecuadas para las TID siempre que incluyan pero compromisos vinculantes y aplicables por parte del responsable o encargado del tratamiento en el tercer país en beneficio de los interesados.

IV

Hechas estas consideraciones iniciales, resulta también procedente determinar cuál será el régimen aplicable a los tratamientos que respecto a los datos personales transferidos puedan llevar a cabo las oficinas exteriores de la entidad en su condición de importadoras de estos datos.

El artículo 3.1 del RGPD dispone que “este Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.”

Hay que tener presente, por tanto, que en los tratamientos que puedan llevar a cabo las oficinas exteriores de la entidad sin personalidad jurídica propia (sucursales u oficinas de representación de la entidad) respecto a los datos personales transferidos por esta entidad (ubicada en Cataluña) les resultará de aplicación las previsiones del RGPD.

El artículo 3.2 del RGPD también dispone que “el presente Reglamento se aplica al tratamiento de datos personales de interesados que se encuentren en la Unión por parte de un responsable u encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas cono:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a éstos se les requiere su pago, (...).”

Por tanto, el RGPD también resultará de aplicación a los tratamientos que respete los datos personales transferidos por la entidad (relativos a interesados que se encuentren en la Unión) puedan llevar a cabo sus oficinas exteriores que tienen personalidad jurídica propia (ubicadas fuera) del EEE), que se efectúen para ofrecer o prestar a ciudadanos que se encuentren en la Unión sus servicios en materia de promoción empresarial.

V

Procede, a continuación, examinar los instrumentos concretos aportados por la entidad para acreditar garantías adecuadas para las TID en sus oficinas exteriores.

Dado que, como se ha visto, la entidad realiza dos propuestas, en atención a la naturaleza jurídica de sus oficinas exteriores, se considera conveniente efectuar este examen de forma separada.

Así, en el siguiente apartado (FJ VI) se realizan una serie de consideraciones en el contrato que se pretende formalizar con las oficinas exteriores de la entidad que gozan de personalidad jurídica propia.

A continuación (FJ VII a XII), se realizan una serie de consideraciones en el convenio que se pretende suscribir con las oficinas exteriores de la entidad que no tienen personalidad jurídica propia.

A pesar de esta distinción, dado que, como veremos, ambos instrumentos se fundamentan, o pretenden fundamentarse, en el uso de cláusulas tipos de protección de datos adoptadas por la Comisión, cabe decir que las observaciones efectuadas hacia un instrumento pueden y deben ser mantenidas igualmente en cuenta en el otro, ya la inversa.

VI

Consideraciones respecto al contrato con las oficinas con personalidad jurídica.

Como se ha dicho, el artículo 46.2.c) del RGPD contempla expresamente el uso de las cláusulas tipos de protección de datos adoptadas por la Comisión como instrumento válido para acreditar garantías adecuadas para las TID en terceros países. Por tanto, de formalizarse un contrato en el que se incluyan estas cláusulas tipo, las TID hacia las oficinas exteriores de la entidad que tienen personalidad jurídica propia podrían realizarse.

Hay que tener en cuenta que las cláusulas tipos adoptadas por la Comisión en esta Decisión 2001/497/CE permanecen en vigor hasta que sean modificadas, sustituidas o derogadas por una nueva decisión de la Comisión (artículo 46.5 RGPD). Si esto ocurriera habría que modificar el contrato firmado con estas oficinas, con el fin de incorporar las nuevas cláusulas tipo adoptadas por la Comisión, o bien utilizar alguno de los otros mecanismos a los que se refiere el artículo 46 del RGPD para la TID.

Por otra parte, hay que tener en cuenta que la Decisión 2001/497/CE fue modificada por la Decisión 2004/915/CE, de 27 de diciembre, con la voluntad de introducir un conjunto alternativo de cláusulas contractuales tipo para las TID en terceros países.

Este conjunto alternativo de cláusulas ofrece un nivel de protección de datos equivalente al proporcionado por el conjunto de cláusulas adoptadas por la Decisión 2001/497/CE, si bien empleando mecanismos distintos, en el sentido de flexibilizar los requisitos en materia de auditoría, de precisar las normas que regulan el derecho de acceso, de presentar un régimen de responsabilidad alternativo a lo previsto en la Decisión 2001/497/CE o de incrementar la participación del exportador de los datos en la resolución de las reclamaciones presentadas por los interesados, entre otros aspectos (considerantes 1 a 6 Decisión 2004/915/CE).

Tal y como dispone el artículo 1 de la Decisión 2001/497/CE, en su nueva redacción dada por la Decisión 2004/915/CE, el responsable del tratamiento es libre de escoger uno u otro conjunto de cláusulas contractuales tipo para las TID en terceros países ("CONJUNTO I" o "CONJUNTO II", ambos definidos en el anexo de la Decisión 2001/497/CE).

Sin embargo, hay que tener presente que cada conjunto de cláusulas constituye un todo coherente, de tal modo que, como dispone este artículo 1, no se permite combinar las cláusulas propias de cada conjunto entre sí, ni tampoco modificarlas total o parcialmente.

Sin embargo, teniendo en cuenta que las cláusulas fueron aprobadas de conformidad con la Directiva 95/46/CE, derogada por el RGPD, podría entenderse que sí sería posible su modificación a efectos sólo de adaptarlas a la nueva normativa y mientras la Comisión no lleve a cabo tal modificación.

Asimismo, se puede admitir la posibilidad de que, junto con estas cláusulas tipo de protección de datos adoptadas por la Comisión (sea el “CONJUNTO I” o el “CONJUNTO II”), se incorporen otras cláusulas o garantías adicionales a criterio de las partes firmantes, siempre que no contradigan las cláusulas tipos ni disminuyan los derechos o libertades fundamentales de los interesados.

Así se desprende del considerante 109 del RGPD:

“La posibilidad de que el responsable o el encargado del tratamiento recurran a cláusulas tipo de protección de datos adoptadas por la Comisión o autoridad de control no debe obstar a que los responsables u encargados incluyan las cláusulas tipo de protección de datos en un contrato más amplio, como un contrato entre dos encargados, o a que añadan otras cláusulas o garantías adicionales, siempre que no contradigan, directa o indirectamente, las cláusulas contractuales tipo adoptadas por la Comisión o por una autoridad de control, ni mermen los derechos o libertades fundamentales de los interesados. Se debe ralentizar a los responsables y encargados del tratamiento a ofrecer garantías adicionales mediante compromisos contractuales que complementen las cláusulas tipo de protección de datos.”

Así pues, siempre que dicho contrato, del que no se adjunta copia, incorpore uno u otro conjunto de cláusulas tipos y se cumplan el resto de principios y obligaciones establecidos en materia de protección de datos, podría considerarse que la TID en las oficinas exteriores de la entidad con personalidad jurídica propia podría efectuarse, al ofrecerse garantías adecuadas sobre la base del artículo 46.2.c) del RGPD, sin que se requiera autorización previa por parte de ésta Autoridad.

VII

Consideraciones respecto al convenio con las oficinas sin personalidad jurídica.

Hay que tener en consideración, de entrada, que, en este caso, nos encontramos ante una TID en la que los destinatarios de los datos personales son parte integrante de la entidad responsable del tratamiento (en el escrito de consulta, se llaman sucursales u oficinas de representación).

la entidad propone la formalización de un convenio con estas oficinas pero, dado que no nos encontramos ante sujetos con personalidad jurídica propia que deciden, en condiciones de igualdad, formalizar este convenio, no parece que esta opción encaje en el supuesto previsto en el artículo 46.2.a) del RGPD. Si bien en la transmisión de los datos puedan existir dos actores diferenciados, en el sentido exportador e importador o destinatario de los datos, lo cierto es que no existe otro sujeto con quien formalizar este convenio (muestra de ello son las dudas que manifiesta la propia entidad, que propone 3 opciones diferentes a la hora de determinar el interlocutor con quien firmar este convenio).

Esto parece que debería llevar a descartar que el instrumento propuesto encaje con el supuesto previsto en el artículo 46.2.a) del RGPD.

Dicho esto, es preciso tener en consideración que, con independencia de su denominación, incluso, del formato, el instrumento propuesto contiene una serie de cláusulas de protección de datos que, como apunta la propia entidad, son de similar naturaleza a las establecidas en la Decisión 2001/497/CE.

Esto podría llevar a considerar que, como en el caso anterior, la entidad pretende fundamentar la TID en estas sucursales u oficinas de representación en el uso del instrumento a que se refiere el artículo 46.2.c) del RGPD .

Ahora bien, para que esto sea posible, debe tenerse en cuenta que, como se ha apuntado antes, las cláusulas incorporadas en este instrumento deberían ajustarse en su conjunto a las dispuestas en el anexo de la Decisión 2001 /497/CE, sea el “CONJUNTO I” o bien el “CONJUNTO II”. Esto con independencia de que puedan incorporarse también otras cláusulas o garantías adicionales.

En caso contrario, deberíamos considerar que nos encontramos ante el supuesto previsto en el artículo 46.3.a) del RGPD, esto es el uso de cláusulas contractuales que no corresponden a las cláusulas tipo adoptadas por la Comisión (artículo 46.2. c) RGPD) o por una autoridad de control (artículo 46.2.d) RGPD) y, en consecuencia, sería necesaria la previa autorización de esta Autoridad (artículo 46.3 RGPD y artículo 42.1.a) LOPDGDD).

Dado que, una vez examinado el documento presentado, todo parece apuntar la voluntad de la entidad de acreditar garantías adecuadas con fundamento en las cláusulas tipo adoptadas por la Comisión (artículo 46.2.c) RGPD), se realizan a continuación una serie de consideraciones al respecto.

Apuntar, a la vista de las tres opciones planteadas por la entidad a la hora de determinar el interlocutor con quien firmar el convenio, que, dado que la TID se pretende fundamentar sobre la base del artículo 46.2.c) de el RGPD, puede entenderse que sería suficiente que la firma del convenio se formalizara con el responsable de la oficina exterior sin personalidad jurídica propia (Opción A).

De no ser ésta la vía escogida, debería formalizarse la solicitud de autorización de la TID a través del formulario que se encuentra disponible en el apartado correspondiente a las TID en la sede electrónica de esta Autoridad (<https://seu.apd.cat/>).

VIII

Consideraciones en el clausulado del convenio.

El documento incorpora las cláusulas tipo propias del “CONJUNTO I” definido en el anexo de la Decisión 2001/497/CE, si bien no en su totalidad.

En concreto, incorpora las cláusulas:

- 1a. Definiciones de conceptos.
- 2a. Detalles de la TID. 4a.
- Obligaciones del exportador de datos. 5a.
- Obligaciones del importador de datos.
- 10a. Legislación aplicable.

Reiterar que cada conjunto de cláusulas constituye un todo coherente (artículo 1 de la Decisión 2001/497/CE, en su redacción dada por la Decisión 2004/915/CE), por lo que no

es posible omitir algunas (a excepción del apartado 3 de la cláusula 6a, que es optativo según la propia Decisión 2001/497/CE).

Por tanto, es necesario, si la entidad quiere acogerse a la vía del artículo 46.2.c) del RGPD, que en el convenio consten todas las cláusulas siguientes:

- 1a. Definiciones de conceptos.
- 2a. Detalles de la TID. 3a.
- Cláusula de tercero beneficiario.
- 4a. Obligaciones del exportador de datos.
- 5a. Obligaciones del importador de datos.
- 6a. Responsabilidad. 7a. Mediación y jurisdicción. 8a. Cooperación con las autoridades de control. 9a. Resolución de conflictos.
- 10a. Legislación aplicable.
- 11a. Variación del acuerdo.

Advertir que, de no introducir en el convenio las cláusulas que carecen de esta Decisión 2001/497/CE, la propuesta no podría considerarse un instrumento vinculante en los términos del artículo 46.2.c) del RGPD, siendo necesaria la autorización previa de esta Autoridad para la TID pretendida.

Recuerda, en este punto, que resulta extraño que la mayor parte de las cláusulas omitidas del convenio sean las dirigidas a garantizar a los interesados “derechos exigibles y acciones legales efectivas” a que se refiere el artículo 46.1 del RGPD, especialmente teniendo en cuenta que la entidad plantea específicamente en su escrito de consulta si puede considerarse que la propuesta efectuada (el convenio) comprende estos aspectos.

Como ya se ha dicho, una vez examinado el convenio en su conjunto, se entiende que la voluntad de la entidad no es recurrir a la vía del artículo 46.3.b) del RGPD sino a la de el artículo 46.2.c) del RGPD, esto es fundamentar la TID en el uso de las cláusulas tipo adoptadas por la Comisión. Y, en este sentido, cabe decir que la garantía de derechos exigibles y acciones legales efectivas a los interesados se logra en este caso con la inclusión en el instrumento que se adopte (el convenio) de uno u otro conjunto de cláusulas tipo del anexo de la Decisión 2001/497/CE en su totalidad, dado que estos conjuntos ya incorporan previsiones específicas en este sentido (por ejemplo, la cláusula de tercero beneficiario, la de mediación y jurisdicción, etc.).

Por tanto, reiterar que si la entidad quiere acogerse a la vía del artículo 46.2.c) del RGPD es necesario incorporar al convenio la totalidad de las cláusulas del “CONJUNTO I” del anexo de la Decisión 2001/497/CE.

Aparte de esto, hay que tener en consideración que también es necesario que el contenido de las cláusulas del convenio no difiera sustancialmente de lo establecido por las mismas en la Decisión 2001/497/CE, sin perjuicio de efectuar las variaciones pertinentes a efectos de adaptarlas a la RGPD.

Por este motivo, se realizan las siguientes observaciones respecto a algunas de las cláusulas incluidas en el convenio:

- Cláusula 4a. Obligaciones del exportador de datos.

El apartado a) de esta cláusula prevé que el exportador de datos acuerde y garantiza que el tratamiento “seguirá efectuándose de acuerdo con las normas pertinentes del Estado miembro

de establecimiento del exportador de datos (....)". Debería indicarse, como tales, el RGPD y el LOPDDDD.

El apartado c) de la cláusula señala que "toda transferencia de datos ha sido consentida por parte del interesado o bien ha sido informada a éste, o será informada antes de su realización, indicando que sus datos podrían ser transferidos a un tercer país que no proporcione una protección adecuada".

Esta previsión no concuerda plenamente con la establecida en la cláusula 4a, que dispone que "si la transferencia incluye categorías especiales de datos, se ha informado al interesado, o será informado antes de la transferencia, de que sus datos podrían ser transferidas a un tercer país que no proporcione una protección adecuada."

Recuerda que la TID no podría fundamentarse en el consentimiento explícito previsto en el artículo 49.1.a) del RGPD, dado que, recordemos, la entidad tiene consideración de autoridad pública a efectos del RGPD (FJ VII Dictamen CNS 6/2018). En consecuencia, debería eliminarse esta previsión del apartado c).

• Cláusula 10a. Legislación aplicable.

Esta cláusula indica que el convenio se regirá por las disposiciones del RGPD y "la legislación vigente del Estado miembro de establecimiento del exportador de datos". Debería indicarse, como tal, la legislación española, en concreto, la LOPDDDD.

Aparte de estas observaciones en cláusulas concretas del convenio, cabe decir que, para evitar posibles confusiones, sería conveniente que en las referencias hechas a lo largo del clausulado del convenio a la "autoridad de control" se indicara como tal esta Autoridad .

IX

Consideraciones en el Anexo 1 del convenio.

De acuerdo con la Decisión 2001/497/CE, en este anexo, que forma parte integrante de las cláusulas, debe concretarse la TID que se pretende llevar a cabo. En concreto, debe especificarse información sobre:

- a) El exportador de datos.
- b) El importador de datos.
- c) Los interesados. d) La finalidad de la TID. e) Las categorías de datos. f) Si procede, la merecedora información de especial protección.
- g) Los destinatarios. h) Periodo máximo de conservación.

En línea con lo que se ha sostenido hasta ahora, y una vez visto el contenido del anexo 1 adjuntado al convenio propuesto, sería necesario que éste se ajustase al esquema establecido por la Decisión 2001/497/CE.

Por eso, se recomienda, como cuestión formal, seguir el mismo orden que en el anexo 1 de la Decisión a la hora de concretar los detalles de la presente TID.

Asimismo, en cuanto al fondo de las previsiones que se contemplan, es necesario tener en cuenta las siguientes observaciones:

- Es necesario incorporar a este anexo 1 del convenio los apartados relativos a “Exportador de datos” e “Importador de datos”, dado que se trata de una información exigida por la propia Decisión 2001/497/CE.

- Sería conveniente revisar el apartado “Finalidades del tratamiento”, que debería denominarse “Finalidad de la TID”, dado que las previsiones que se contemplan no resultan suficientemente claras y podrían llevar a confusión.

En este apartado del anexo es necesario especificar la finalidad o los objetivos a los que responde la TID. El apartado describe, por categorías de interesados, lo que se entiende que sería la finalidad principal para la que, en cada caso, se tratarán los datos transferidos y los usos que pudieran derivarse. Ahora bien, no se hace ninguna distinción al respecto. Podría ser conveniente, para facilitar su comprensión, que se especificase sólo los fines principales a los que responderá el tratamiento de los datos transferidos.

- Es necesario revisar el apartado “Bases de legitimación del tratamiento”, dado que las previsiones que se contemplan tampoco resultan suficientemente claras y podrían llevar a confusión.

Debe tenerse presente, de entrada, que éste es un apartado no contemplado específicamente en el anexo 1 de la Decisión 2001/497/CE, por lo que su inclusión en el convenio no resultaría exigible. Sin embargo, dado que, como se ha visto, los responsables pueden añadir otras garantías adicionales para las TID, siempre que no resulten contradictorias con lo establecido en dicha Decisión ni comporten una disminución de los derechos e intereses de los afectados, se puede admitir su incorporación en el convenio. Ahora bien, para que esto sea así, es necesario que quede suficientemente claro a lo que responde su inclusión.

El apartado indica que “el tratamiento de los datos transferidos con las finalidades referenciadas anteriormente se encuentra legitimado en base a” y, a continuación, detalla cuáles son estas bases jurídicas. Ahora bien, no indica ni tampoco se desprende claramente a quien corresponde ese tratamiento.

Puede entenderse, dado el contexto en el que nos encontramos, que se informa de las bases que legitiman los tratamientos que puedan llevar a cabo las oficinas de representación o sucursales de la entidad a partir de los datos personales transferidos. Pero, siendo así, habría que indicarlo claramente, porque si no podría pensarse que se refiere a la base que legitima el tratamiento de estos datos en origen, es decir, por el exportador de datos (la entidad) y ésta es una información a la que no es necesario hacer referencia en el convenio.

- Revisar los apartados “Cesiones y legitimación” y “Transferencia internacionales y legitimación” y, en su caso, refundirlos en un único apartado, que debería llamarse “destinatarios”.

Es necesario especificar en el anexo 1 del convenio la existencia (o no) de comunicaciones posteriores de los datos personales transferidos por parte del importador de datos (las sucursales u oficinas de representación de la entidad), o lo que es lo mismo los destinatarios o categorías de destinatarios de estos datos.

Los apartados “Cesiones y legitimación” y “Transferencia internacionales y legitimación” del convenio parecen referirse a esta cuestión pero las previsiones que se contemplan no resultan suficientemente claras.

De entrada, no está claro por quiénes serían llevadas a cabo las comunicaciones de datos a las que se hace mención. Como se ha dicho, es necesario concretar si el importador (las oficinas) puede comunicar los datos objeto de la TID ya quién, en atención a los destinatarios especificados (especialmente en el apartado “Cesiones y legitimación”), se podría hacer pensar que, en realidad, se está haciendo

en las comunicaciones propias del exportador (la entidad). De ser así, hay que tener presente que ésta es una información que no debería recogerse en un documento como el que se examina. Por tanto, habría que revisar estos apartados para esclarecer esta cuestión.

Para el caso de que sí se esté haciendo referencia a las comunicaciones de datos por parte del importador, aparte de mejorar la redacción para evitar confusiones como la apuntada, es necesario advertir de una posible contradicción entre estas previsiones y lo establecido en el anexo 2 del convenio.

De acuerdo con estos apartados del anexo 1, el importador (las oficinas) podría comunicar los datos personales transferidos a diversas categorías de destinatarios. Ahora bien, si nos atendemos en el punto 5 del anexo 2, en el que se recoge la obligación de no divulgar, transferir o comunicar por cualquier otra forma los datos personales a los que se tenga acceso, ni siquiera para su conservación, se prevé lo contrario. Por tanto, también habría que aclararlo.

Por otra parte, tampoco está claro a qué obedece la distinción entre categorías de destinatarios que se hace en estos apartados del anexo 1.

En el apartado "Cesiones y legitimación" se engloban, por un lado, administraciones públicas, proveedores de servicios, empresas de auditoría, y fuerzas y cuerpos de seguridad y, por otro, entidades o empresas interesadas en la obtención de servicios de internacionalización o que colaboren con la entidad.

En el apartado "Transferencia internacionales y legitimación" se engloban, por un lado, las oficinas de representación de la entidad -que, como veremos, no deberían incluirse- y los proveedores de servicios y, por otro, las entidades o empresas interesadas en la obtención de servicios de internacionalización o que colaboren con la entidad.

Sería conveniente esclarecer el motivo de estas distinciones (por ejemplo, si se trata de diferenciar encargados del tratamiento de otros terceros destinatarios de los datos).

Además, resulta especialmente confuso que en el apartado Transferencia internacionales y legitimación se haga referencia a las propias oficinas de representación de la entidad, dado que éstas ocuparían la posición del importador de datos.

No debe confundirse el destinatario de los datos objeto de la TID por la entidad, esto es las oficinas de representación, con lo que sería un destinatario de una posible comunicación posterior de estos datos por parte del importador (que es la información que debe concretarse en el anexo 1). Por tanto, habría que eliminar esta referencia a dichas oficinas.

En definitiva, es necesario revisar ambos apartados de este anexo 1 del convenio con el fin de identificar claramente la existencia o no de restricciones en la transmisión ulterior de datos por parte del importador y los destinatarios de estas transmisiones.

Dicho esto, a la vista de los posibles destinatarios de los datos (como constan en el anexo 1), entre ellos proveedores de servicios y empresas de auditoría, incluso, otras empresas que "colaboran con la entidad", recuerda la conveniencia de prever en el convenio, si procede, la formalización con éstos de un contrato de encargado del tratamiento en los términos establecidos en el artículo 28.3 del RGPD.

Recordar, en este punto, que el importador de datos está sometido al RGPD en lo que se refiere a los tratamientos relacionados con la TID examinada. Por tanto, cualquier comunicación de los datos recibidos como consecuencia de esta TID, sea a un tercero o no (artículo 4.10 RGPD), deberá contar con legitimación suficiente (artículo 6 RGPD).

- Revisar el apartado "Periodo de conservación de los datos".

En este apartado se especifica el período máximo durante el cual el importador podrá conservar los datos personales transferidos, tal y como exige la Decisión 2001/497/CE, en los siguientes términos:

- Con respecto a los datos de candidatos a procesos de selección: 2 años.
- En cuanto a los datos del resto de categorías de interesados: mientras se mantenga la relación, según el caso, laboral, contractual o jurídica con el interesado y, una vez finalizada, "durante los plazos de prescripción legales de aplicación y/o los plazos necesarios para garantizar la misión de interés público de la entidad y los plazos necesarios para acreditar el cumplimiento de las obligaciones legales o contractuales de la entidad".

Recuerda que la previsión de conservar los datos durante "los plazos necesarios para acreditar el cumplimiento de las obligaciones legales" resulta redundante, dado que también se prevé que se conservarán durante "los plazos de prescripción legales de aplicación". Por tanto, debería modificarse.

Dicho esto, sería bueno que se concretara, en la medida de lo posible, cuáles serían estos plazos a los que se hace mención, teniendo en cuenta que los datos remitidos no deberían conservarse durante más tiempo del necesario para alcanzar la finalidad a la que responde la TID.

X

Consideraciones en el Anexo 2 del convenio.

Siguiendo el modelo establecido en la Decisión 2001/497/CE, en el anexo 2 a las cláusulas contractuales tipo se recogen los principios que el importador debe respetar en el tratamiento de los datos personales enviados, de conformidad con lo establecido en la cláusula 5.b) (obligaciones del importador). En concreto:

1. Limitación de la finalidad.
2. Calidad y proporcionalidad.
3. Transparencia.
4. Seguridad y confidencialidad.
5. Derechos de acceso, rectificación, supresión y bloqueo de datos.
6. Restricciones a la transferencia ulterior.
7. Categorías especiales de datos.
8. Marketing directo.
9. Decisión individual automatizada.

De acuerdo con la Decisión 2001/497/CE, estos principios deben regirse e interpretarse de acuerdo con lo establecido en la Directiva 95/46/CE. Esta Directiva ha sido derogada por el RGPD, con lo que hay que entender que dichos principios deberán interpretarse a la luz de la nueva regulación.

Como se ha visto, las cláusulas tipo adoptadas por la Comisión por medio de esta Decisión y, por tanto, también sus anexos, permanecen vigentes hasta que sean modificadas, sustituidas o derogadas por una nueva decisión de la Comisión (artículo 46.5 RGPD).

Por tanto, en principio las previsiones establecidas en el anexo 2 del convenio deberían adecuarse a las establecidas en la Decisión, tanto en lo que se refiere a la denominación de los apartados relativos a los principios como a su contenido. Sin embargo, se podría admitir una adaptación y amp

efectos de adecuarlas a la nueva regulación. Pero, en cualquier caso, por ahora no es posible omitir alguna.

El anexo 2 del convenio no incluye la totalidad de los principios establecidos en la Decisión 2001/497/CE, por lo que es necesario incluir las previsiones sobre:

- “Restricciones en la transferencia ulterior” de datos (apartado 6).
- “Marketing directo” (apartado 8).
- “Decisión individual automatizada” (apartado 9).

De no hacerlo, como se ha visto, no podría considerarse que el instrumento propuesto responde al mecanismo establecido en el artículo 46.2.c) del RGPD y sería necesaria la autorización previa de esta Autoridad, o bien acogerse a uno de los otros mecanismos del artículo 46 del RGPD, para efectuar la TID.

Asimismo, teniendo en cuenta las previsiones del RGPD, debería añadirse también al anexo 2 del convenio el principio de “responsabilidad proactiva” (artículo 5.2). En este sentido, podría indicarse que el importador de datos será responsable del cumplimiento de estos principios y que aplicará medidas técnicas y organizativas apropiadas, a fin de garantizar y poder demostrar que el tratamiento de los datos transferidos es conforme al RGPD .

Dicho esto, se examinan las previsiones que constan en el anexo 2 del convenio, efectuando algunas observaciones al respecto.

1. Limitación de la finalidad.

Se establece que los datos se tratarán, emplearán o transferirán sólo para las finalidades concretas expresadas en el anexo 1 del convenio. Se infiere, por tanto, que el importador (sucursal u oficina de representación) no podrá utilizarlas para otros hasta que resulten incompatibles con éstos (artículo 5.1.b) RGPD).

Asimismo, siguiendo la Decisión 2001/497/CE, se establece que no se conservarán durante más tiempo que el necesario, previsión que responde al principio de limitación del plazo de conservación (artículo 5.1.e) RGPD).

2. Calidad y proporcionalidad de los datos.

Se establece que los datos serán precisos y, en caso necesario, se mantendrán actualizados, previsión que responde al principio de exactitud (artículo 5.1.d) RGPD).

A continuación, se establece que los datos serán adecuados, pertinentes y no excesivos en relación con la finalidad de su transferencia y tratamiento posterior (artículo 5.1.c) RGPD).

Hay que entender, por tanto, que el exportador (la entidad) sólo transferirá al importador (la sucursal) datos personales exactos y actualizados que, a su vez, serán los mínimos necesarios para alcanzar la finalidad para la que se le transfieren. También puede entenderse que cada uno de ellos informará al otro en caso de tener conocimiento de que los datos personales transferidos son inexactos, a efectos de proceder ambos a su rectificación.

3. Transparencia.

Se establece que será necesario facilitar a los interesados información sobre el tratamiento de sus datos de conformidad con lo establecido en los artículos 13 y 14 del RGPD, y en cumplimiento del principio de transparencia del artículo 12 del RGPD.

Sin cuestionar que esto sea correcto, cabe decir que se trata de una previsión poco precisa. En este apartado es importante que se concrete, de forma clara, cómo se informará al interesado y, en este sentido, las previsiones establecidas en el anexo 2 de la Decisión 2001/497/CE resultan más esclarecedoras.

Por este motivo, se sugiere modificar la actual redacción de este apartado en la línea de lo establecido en dicha Decisión, por ejemplo, indicando que “se facilitará a los interesados información sobre la finalidad del tratamiento y la identidad del responsable del tratamiento de los datos en el tercer país, así como el resto de información a la que se refiere el artículo 14 del RGPD, salvo que ya lo haya proporcionado el exportador de datos de conformidad con el artículo 13 del RGPD” o algo similar.

4. Seguridad.

Se recogen las mismas previsiones que el artículo 32 del RGPD, apartados 1 y 2. Asimismo, se prevé que, como mínimo y en cualquier caso, se adoptarán las medidas de seguridad identificadas en el anexo 3 del convenio (a que se hace mención más adelante).

Hay que entender, por tanto, que el importador (la sucursal) se compromete a aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que pueda comportar el tratamiento de los datos remitidos, especialmente, para protegerlos contra el acceso accidental o ilícito, la destrucción, pérdida, alteración o divulgación no autorizada (artículo 5.1.f) RGPD).

5. Confidencialidad, control y custodia.

Se establece que las personas que actúen bajo la autoridad de “los responsables”, incluido el encargado, no tratarán los datos para finalidades distintas de las referenciadas en el anexo 1 o sin la observancia de las instrucciones del responsable. Asimismo, se establece que estas personas deberán mantener el deber de secreto respecto a los datos a los que tengan acceso, incluso después de finalizar la relación que mantienen con el responsable, comprometiéndose por escrito.

Por otra parte, se establece que “los responsables” tendrán que guardar bajo su control y custodia los datos personales a los que acceda “con motivo de la prestación del servicio” y que no los divulgarán, transferirán o comunicarán de cualquier otra forma, ni siquiera para su conservación, a otras personas ajenas al mismo.

Es necesario modificar la referencia hecha en plural al responsable, dado que en este anexo, como se ha dicho, es necesario concretar de forma clara los principios a los que el importador de datos queda sujeto en el tratamiento de los datos transferidos, en este caso en materia de seguridad de la información. La referencia hecha a los “responsables” podría llevar a pensar que esta previsión se dirige también al exportador. Si bien es cierto que la entidad también debe adoptar las medidas de seguridad que resulten oportunas respecto a los datos de los que es responsable, no es pertinente incluirlo en el presente anexo.

Asimismo, a fin de evitar posibles confusiones, sería conveniente modificar la expresión “con motivo de la prestación del servicio” del segundo párrafo de este apartado del anexo 2 por “con motivo de la TID”.

Dicho esto, debería refundirse este apartado con el anterior (llamado seguridad), dado que las previsiones contenidas en ambos apartados están relacionadas con el principio de integridad y confidencialidad (artículo 5.1.f) RGPD).

6. Notificación de violaciones de seguridad, EIPD y consultas previas.

Se establece que cuando el importador tenga conocimiento de una violación de seguridad de los datos personales enviados informará sin dilación indebida al exportador (la entidad), así como que le asistirá en la notificación de esta violación a ésta Autoridad u otra autoridad de control competente y, en su caso, a los interesados afectados por esta violación.

También se establece que el importador apoyará al exportador en la realización de evaluaciones de impacto de privacidad y en la consulta previa a esta Autoridad u otra competente cuando sea procedente.

Se trata de una serie de previsiones no contempladas expresamente en el anexo 2 de la Decisión 2001/497/CE, pero puede admitirse su pertenencia a la luz del RGPD.

7. Derechos de los interesados.

Se establece que las partes velarán y garantizarán el ejercicio de los derechos de los interesados regulados en el RGPD, así como que el importador asistirá al exportador para que éste pueda cumplir con la obligación de dar respuesta a las solicitudes de ejercicio de derechos.

Esta previsión hay que decir no está suficientemente clara. Es necesario que en este apartado se establezca de forma clara que el importador atenderá las solicitudes de ejercicio de derechos que los interesados puedan dirigirle en relación con los tratamientos de los datos personales de los que sea responsable. Y, respecto a aquellos tratamientos de datos de los que sea responsable el exportador de datos, es necesario establecer que el importador le asistirá para que éste pueda atender correctamente las solicitudes de ejercicio de derechos por parte de los interesados.

Por otra parte, no se contempla la posibilidad de que el interesado pueda recabar la tutela de esta Autoridad en caso de que sus derechos no sean atendidos. Habría que incluir, por tanto, una previsión en este sentido, a efectos de garantizar correctamente el ejercicio de estos derechos.

8. Registro de las Actividades de Tratamiento.

En este apartado se establece que el importador debe auxiliar al exportador en la realización y actualización de su RAT, informándole sobre las actividades de tratamiento que está llevando a cabo o que proyecte llevar a cabo.

No está claro a qué obedece una previsión de este tipo, teniendo en cuenta que la obligación de llevar a cabo el RAT corresponde a cada responsable del tratamiento (artículo 30 RGPD). En cualquier caso, dado que no responde a ningún principio de protección de datos, debería eliminarse del anexo 2 del convenio.

9. Privacidad desde el diseño y por defecto.

Se establece que el importador, siempre que proyecte llevar a cabo nuevas operaciones de tratamiento, debe informar al exportador de su diseño e implantación, a fin de aplicar los principios de protección de datos desde el diseño y por defecto conforme lo establecido en el artículo 25 del RGPD.

Se trata de una previsión no contemplada expresamente en el anexo 2 de la Decisión 2001/497/CE, pero puede admitirse su pertenencia a la luz del RGPD. Tan sólo recuerda que el principio a que se hace mención es "protección de datos desde el diseño y por defecto", por lo que habría que modificar la denominación de este apartado.

XI

Consideraciones en el Anexo 3 del convenio.

El convenio incorpora un anexo en el que se establece el compromiso de ambas partes (exportador e importador) de aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para la protección de los derechos y libertades de las personas físicas.

Este anexo no está contemplado expresamente en la Decisión 2001/497/CE, si bien puede entenderse que se inserta con voluntad de concretar o desarrollar las previsiones establecidas en el anexo 2 de esta Decisión (y del convenio) sobre el principio de seguridad (apartado 4).

A tal efecto, se establece, a todos los efectos, una serie de medidas de seguridad y para los tratamientos que se identifiquen como “especialmente sensible”, que, hay que entender, de mayor riesgo, una serie de medidas adicionales.

Recuerda que, en la definición y la implantación del conjunto de medidas de seguridad descritas en este anexo, habría que tener en consideración, entre otros instrumentos en materia de seguridad informática (estándares internacionales y/o certificaciones, por ejemplo), también los criterios establecidos en el Esquema Nacional de Seguridad, aprobado por Real Decreto 3/2010, de 8 de enero (que, actualmente, está siendo objeto de revisión).

Así se desprende de las previsiones establecidas en la disposición adicional primera de la LOPDGDD:

“Disposición adicional primera. Medidas de Seguridad en el ámbito del sector público.

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos de carácter personal, para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de las datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetos al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.”

De acuerdo con este precepto, los sujetos enumerados en el artículo 77.1 de la LOPDGDD, entre ellos, las administraciones de las comunidades autónomas, deben procurar que sus empresas o fundaciones implementen medidas de seguridad equivalentes a las propias, las cuales se deben adecuar necesariamente a los criterios establecidos en el ENS.

Dado que, en el presente caso, la entidad es una entidad de derecho público que se sujeta al derecho privado dependiendo de la Administración de la Generalidad (artículo 77.1.d) LOPDGDD), las medidas de seguridad que se implementen en organización, con independencia de la ubicación de sus oficinas, deberían ajustarse también al ENS.

XII

Llegados a este punto, cabe decir que, siempre que se adopten los cambios pertinentes a efectos de adaptar el convenio y sus anexos a la Decisión 2001/497/CE (CONJUNTO I) y al RGPD (mencionados a lo largo de los FJ VII a XI de este dictamen), podría considerarse que se aportarían garantías adecuadas para la TID en las oficinas de representación o sucursales de la entidad ubicadas en terceros países no cubiertos por una decisión de adecuación de la Comisión.

En consecuencia, también podría considerarse que la TID planteada por la entidad podría efectuarse sobre la habilitación conferida en el artículo 46.2.c) del RGPD, sin que se requiera la autorización previa de esta Autoridad .

De acuerdo con las consideraciones hechas hasta ahora en relación con la consulta planteada, se hacen las siguientes,

Conclusiones

La TID respecto a las oficinas exteriores de la entidad en base a las cláusulas tipo de protección de datos adoptadas por la Comisión en la Decisión 2001/497/CE, de 15 de junio de 2001, estaría legitimada por el artículo 46.2.c) del RGPD, siendo pero necesario que los instrumentos en los que se incorporen estas cláusulas se adecuen a dicha Decisión y al RGPD, en los términos apuntados en este dictamen.

Barcelona, 9 de abril de 2019