EasyTelecom Law Firm
Soluciones legales para tu negocio

ASPECTOS A TENER EN CUENTA POR LAS ADMINISTRACIONES PÚBLICAS EN LA CONTRATACIÓN DE SERVICIOS DE *CLOUD COMPUTING*

1. Introducción.

Tras la revisión de los pliegos de licitación de contratación de *cloud computing*, se aprecian ciertas deficiencias por cuanto que, en ocasiones, en las bases de licitación no se exigen requisitos que acrediten el cumplimiento de la normativa en materia de protección de datos y en materia de seguridad de la información por parte de los prestadores de servicios de computación en la nube. Por ello, se elabora el presente documento en el que se indicarán diferentes recomendaciones que podrían ser tomadas en consideración por las Administraciones Públicas (AAPP), dado que las mismas son responsables del tratamiento de datos personales.

2. Recomendaciones.

De acuerdo con la Guía, publicada por la Agencia Española de Protección de Datos (AEPD)[1], relativa a la contratación de servicios de computación en la nube, las AAPP gestionan un volumen considerable de datos de los ciudadanos con la consecuencia de que las mismas deben adoptar ciertas salvaguardas para evitar que los derechos de los propios ciudadanos se vean comprometidos.

A fin de evitar tales riesgos, los pliegos de prescripciones deberían hacer referencia a los siguientes aspectos:

a) La diligencia del prestador de servicios de *cloud computing*, puesto que tendrá la consideración de encargado del tratamiento, que deberá cumplir las obligaciones dispuestas en el artículo 28 del RGPD, que en definitiva, consisten en ofrecer garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

b) El prestador debe realizar un tratamiento de los datos teniendo en cuenta las instrucciones de carácter documental proporcionadas por el responsable del tratamiento, es decir, la Administración Pública. Las Administraciones tienen en consideración los tipos de servicios el proveedor ofrece, y pueden seleccionar cual o

[1] Agencia Española de Protección de Datos. (2018). *Guía para clientes que contraten servicios de cloud computing*. https://www.aepd.es/sites/default/files/2019-09/guia-cloud-clientes.pdf

cuales ofrecen garantías adecuadas en materia de protección de datos y que cumplan con los servicios requeridos.

c) La Administración Pública, necesariamente debe suscribir un contrato formal de encargado del tratamiento con el proveedor de servicios que contrate (no podrá considerarse válido un acuerdo informal, bajo el criterio de la AEPD), indicando el objeto, naturaleza y finalidad del tratamiento en la prestación de sus servicios, así como la tipología de datos personales, categorías de interesados, y los derechos y obligaciones del propio responsable, según el artículo 28.3 del RGPD.[2]

d) En virtud del contrato de encargado del tratamiento con la Administración Pública, el proveedor de cloud deberá cumplir el deber de diligencia en lo relativo a informar de manera transparente al responsable del tratamiento, estipulado en el artículo 28.3 letra h), el encargado del tratamiento debe demostrar el cumplimiento de sus obligaciones así como permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable. Esta última obligación resulta muy relevante puesto que, encontramos en determinados pliegos que las Administraciones contratantes realizarán auditorías periódicas a los adjudicatarios. En definitiva, la transparencia configura un principio esencial que debe presidir las relaciones entre las partes.

e) En varias licitaciones se han encontrado obligaciones adicionales que las Administraciones exigen a los proveedores de servicios cloud, en lo relativo al ejercicio de los derechos de los interesados, reconocidos legalmente por parte de los interesados, si bien el responsable del tratamiento (la Administración Pública), está obligado a facilitar el ejercicio de estos derechos reconocidos en los artículos del 15 al 22 del RGPD en los plazos legalmente establecidos, es posible que se precise la colaboración del encargado del tratamiento en una contratación pública. Por tanto, el proveedor de cloud, en una licitación debe prever que pueda ser necesaria esta colaboración.

f) Tanto la Administración responsable del tratamiento de los datos personales, como el licitador encargado del tratamiento, deben cumplir el RGPD respecto a las transferencias de datos internacionales. Por ello, las Administraciones, deben asegurarse que los contratistas están situados en la Unión Europea tanto los servidores y sistemas de almacenamiento, como los backups u otros servicios que dispongan y traten datos personales derivados de la contratación. Asimismo, los contratistas deben

[2] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

asegurarse que estas mismas condiciones se cumplan para los subcontratistas con los que puedan colaborar en la prestación de los servicios.

La prestación de servicios de cloud, por la naturaleza de los servicios, implica flujos de datos, y las Administraciones Públicas deben prestar especial atención cuando estos son transmitidos a terceros países. Dadas las características propias de los servicios de *cloud computing*, es necesario que las Administraciones, si prevén subcontrataciones, es necesario que establezcan mecanismos para permitir que estas puedan realizarse, teniendo especial consideración las transferencias internacionales a terceros países, y se aseguren que se ofrecen las garantías suficientes para realizar transferencias de datos de forma segura asegurando al mismo tiempo que las Administraciones Públicas disponen de información suficiente sobre los subcontratistas, o potenciales subcontratistas, y mantiene en todo momento la capacidad de tomar decisiones.[3]

g) Las Administraciones Públicas en sus licitaciones, deben exigir el cumplimiento de las medidas técnicas y organizativas estipuladas en el artículo 32 RGPD, para que el tratamiento de datos se realice de forma segura, para garantizar un nivel de seguridad adecuado al riesgo, estos requisitos para la seguridad del tratamiento son generalistas y no se estipula un listado de medidas, únicamente, en virtud de la responsabilidad proactiva del responsable y encargados, estos deberán garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

   A raíz del análisis de los pliegos administrativos, podemos confeccionar un listado de las medidas más requeridas por las Administraciones Públicas:

   1) Encriptación y seudonimización de datos: Las Administraciones Públicas requieren que los datos deben ser almacenados y transmitidos en la nube de forma encriptada para protegerlos contra accesos no autorizados.
   2) Autenticación y acceso seguro: Se deben implementar medidas de autenticación robustas, como contraseñas fuertes, autenticación de dos factores (2FA) y certificados digitales, para asegurar que solo las personas autorizadas tengan acceso a los datos.
   3) Seguridad de la infraestructura: Las entidades públicas licitadores suelen exigir que el proveedor cuente con medidas de seguridad físicas y lógicas para proteger sus centros de datos y la infraestructura de red.

[3] Orientaciones para Prestadores de Servicios de Cloud Computing
https://www.aepd.es/es/documento/guia-cloud-prestadores.pdf

4) Copias de seguridad y backups: Se deben establecer procedimientos para realizar copias de seguridad regulares y garantizar la recuperación de datos en caso de un incidente.
5) Monitorización y detección de intrusiones: se debe contar con sistemas de monitorización y detección de intrusiones para identificar actividades sospechosas y responder rápidamente a posibles ataques.
6) Actualizaciones y parches de seguridad: El proveedor debe mantener sus sistemas actualizados con las últimas correcciones y parches de seguridad para mitigar vulnerabilidades conocidas.
7) Políticas de gestión de incidentes: Deben establecerse procedimientos para gestionar y notificar adecuadamente cualquier incidente de seguridad que pueda afectar a los datos de los clientes.
8) Cumplimiento y auditorías: El proveedor debe someterse a auditorías periódicas para asegurar el cumplimiento de las normativas y estándares de seguridad aplicables. Estas auditorías, podrán ser practicadas por los propios licitadores o terceros que los licitadores nombren para realizarlas.[4]

h) El prestador de servicios Cloud, también debe demostrar diligencia y compromiso con la ciberseguridad, aunque en algunos pliegos de los analizados no se establece un listado de cumplimiento normativo en materia de ciberseguridad, las Administraciones si lo desean, pueden requerir una serie de responsabilidades para la prestación del servicio, las cuales las podemos englobar en:
   i) Respecto a cumplimiento normativo, principalmente, se requiere el cumplimiento de:
      1) Esquema Nacional de Seguridad.
      2) Esquema Nacional de Interoperabilidad.
      3) ISO 27001.
   ii) Complementariamente, en en determinados pliegos, se encuentra el requisito de cumplimiento de:
      1) ISO 27017 de seguridad nube.
      2) ISO 27018 de privacidad nube.

i) Las Administraciones Públicas, deben exigir, una vez finalizada la relación contractual, que los datos que hayan tratados por el proveedor de los servicios cloud que estos sean devueltos a la Administración y, adicionalmente, el proveedor deberá proceder a la destrucción de los mismos de forma completa e irreversible, por lo que,

[4] Pliego para la Renovación y ampliación del clúster IaaS en modo nube privada de entornos de desarrollo y laboratorios Expediente 053/23. pp 15-17
https://contrataciondelestado.es/wps/wcm/connect/e8132762-204e-407f-83e9-d7c4cb263858/DOC20230721115938053_23_PCT_Renovacion_ClusterIaaS_NubePrivadaLabs_corregido.pdf?MOD=AJPERES

de conformidad con el artículo 5.1.f) del RGPD la Administración puede solicitar un certificado de destrucción de datos, tanto en formato físico como digital.[5]

j) Respecto a la subcontratación, la validez de la misma se supedita a la concurrencia de tres requisitos: primero, que el contrato entre responsable y encargado del tratamiento estipule expresamente dicha posibilidad; segundo, que el tratamiento de datos personales se adecúe a las instrucciones de la entidad contratante (responsable del tratamiento) y, tercero, que el prestador de servicios de computación en la nube y el tercero (subencargado) formalicen un contrato.

   Cabe destacar que, a medida que evoluciona la contratación de los servicios de *cloud computing*, así como incrementa el compromiso de realizar transferencias internacionales seguras por parte de los licitadores, la Administración debe autorizar cualquier subcontratación por parte del proveedor de servicios de *cloud computing*, y para que sea concedida, los subcontratistas deberán estar situados en el territorio de la Unión Europea, y en caso que la Administración no autorice la subcontratación, o los subcontratistas estén situados en terceros países fuera de la UE, será motivo para rescindir el contrato.

k) Las Administraciones Públicas, deben prever que el contenido del contrato de prestación de servicios de *cloud computing* debe incluir aquellas medidas de carácter técnico y organizativo que el prestador de dichos servicios tiene previsto adoptar. Además, la disponibilidad, integridad y confidencialidad que puede exigir un servicio electrónico determinado prestado por la Administración Pública, en concreto, una sede electrónica, se garantizará a través de la previsión en el contrato de un acuerdo de nivel de servicio (SLA[6]). En este caso, dicho acuerdo especificará los indicadores de calidad de servicio que serán objeto de medición así como los valores mínimos de los mismos que se considerarán aceptables.

Igualmente, aunque, según el artículo 62 de la LCSP[7], corresponde a los órganos de contratación la designación de un responsable del contrato que asegure la correcta realización de la prestación pactada, dicho nombramiento no modifica las responsabilidad y obligaciones a las que está sujeto el responsable del tratamiento de conformidad con la normativa de protección de datos personales.

---

[5] A la luz del RGPD la destrucción de datos, tiene la consideración de tratamiento: Art. 4.2 RGPD "*«tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, (...) supresión o destrucción;*"

[6] Service Level Agreement, por sus siglas en inglés.

[7] Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

Por otra parte, en relación con el Esquema Nacional de Seguridad, la AEPD destaca que la contratación de esta clase de servicios tiene un impacto directo en ciertos aspectos del Esquema:

1. Análisis y gestión de riesgos. Es decir, la contratación de estos servicios requiere un análisis de riesgos previo.

2. Protección de la información almacenada y en tránsito. Será preciso que el contrato de prestación de servicios de *cloud computing* establezca medidas de seguridad, tales como "*la aplicación de técnicas robustas de cifrado a los datos en tránsito y en almacenamiento*"[8] y "*la realización de copias de respaldo*"[9].

3. Incidentes de seguridad y continuidad de actividad. Se requiere una gestión de los incidentes de seguridad que otorgue garantías para que la actividad pueda ser desarrollada aun cuando se produzcan catástrofes.

4. Auditorías de seguridad. Esto es, garantizar la realización de auditorías de seguridad tanto ordinarias como extraordinarias.

Finalmente, la ubicación de los datos personales es determinante puesto que el país en el que se encuentren ubicados, determinará la aplicación de una normativa que ofrezca mayores garantías o no. Por ello, si los datos personales fueren almacenados en países que no pertenecen al Espacio Económico Europeo[10], se estaría realizando una transferencia internacional de datos lo que requiere, a su vez, la adopción de garantías adicionales.

3. Anexo a incluir en el pliego de cláusulas administrativas particulares.

Con arreglo a lo expuesto anteriormente, se considera recomendable establecer que en el pliego de cláusulas administrativas particulares uno o varios anexos relativos a la protección de datos personales. En este caso, cabe traer a colación el previsto en el pliego de cláusulas administrativas particulares del Ministerio de Defensa referido a la contratación de un proyecto de establecimiento de comunicaciones basadas en tecnología 5G[11], dado que algunas de sus previsiones podrían resultar aplicables a la contratación de servicios de computación en la nube.

[8] AEPD, ob. cit.
[9] *id.*
[10] Dicho Espacio engloba a los países de la Unión Europea, Islandia, Liechtenstein y Noruega.
[11] Pliego de cláusulas administrativas particulares que ha de regir la contratación del proyecto de establecimiento de comunicaciones basadas en tecnología 5g en diversas unidades la armada https://contrataciondelestado.es/wps/wcm/connect/b71f8480-f916-4b06-809e-31e88f9634f3/DOC20230131125111109+PCAP+v20221219.pdf?MOD=AJPERES.

Así, por ejemplo, se incluye un Anexo ("*Anexo XV de Protección de Datos de Carácter Personal en contratos que impliquen un tratamiento de datos por el contratista*"[12]), según el cual, se dispone una declaración por parte del prestador de servicios de la ubicación de los servidores, así como desde qué lugar se prestarán los servicios contratados y si dicho prestador tiene previsto la subcontratación de sus servicios. Luego, se acompaña un Anexo ("*Anexo XVI Declaración ubicación servidores Protección de Datos*"[13]) en el que el prestador de servicios ha de indicar si es titular o no de los servidores y, en caso de que contrate los servicios de alojamiento a un tercero, se recogerá la identidad de dicho tercero, su ubicación y localidad en la que está radicado.

Además, en relación con el párrafo anterior, se menciona en el pliego de las prescripciones técnicas para la Contratación del suministro de licencias de una Suite ofimática basada en Cloud Computing[14], de Costa del Sol, establece, en el apartado de características de seguridad, que el servicio prestado debe cumplir con la totalidad de la normativa aplicable española y europea sobre datos de carácter personal, en particular los requisitos relativos a la transferencia internacional de datos.

Tal y como se comentó anteriormente, la entidad pública contratante podría proporcionar un contrato de encargado del tratamiento al prestador de servicios de *cloud computing*, especificando si se permite a este último la subcontratación de los servicios o no y, en caso de que se permita, será dicha entidad la que deberá autorizar dicha subcontratación por escrito, conforme al artículo 28.2 del RGPD. Por tanto, se podría prever el plazo durante el cual el responsable del tratamiento (entidad contratante) puede manifestar su oposición a la subcontratación por parte del encargado del tratamiento.[15]

En definitiva, las Administraciones Públicas al elaborar las bases de los pliegos de las licitaciones de los servicios de *cloud computing*, deberán tener en cuenta dos puntos principales:

- No todos los servicios y proveedores de cloud computing son iguales, pero siempre debe realizarse bajo un contrato de encargado del tratamiento regulado en el artículo 28 RGPD.
- La responsabilidad por incumplimiento de la ley puede exigirse a las Administraciones contratantes así como al prestador de servicios por igual, sin

[12] *ibid*, pp. 151-158.
[13] *ibid*., pp. 159-162.
[14] PLIEGO DE PRESCRIPCIONES TÉCNICAS DE PRITIA-CLOUD https://contrataciondelestado.es/wps/portal/!ut/p/b0/Dco7CoAwDADQIwUVQQUHBycFJz_tIsHEEk2rQ_H8dnzwwMIGNuAnDqM8ATXZEPOrEu6GOKIq7yqHRDxSgBUsWKH-UzBX7ubCZ9NEJQ-OqvFcltq1Lbzedz8V7KwU/
[15] AEPD. (2018). Directrices para la elaboración de contratos entre responsables y encargados del tratamiento. https://www.aepd.es/es/documento/guia-directrices-contratos.pdf

embargo, en lo relativo a las transferencias de datos internacionales aunque se realicen a través de subcontrataciones, el proveedor de servicios tendrá la consideración de responsable del tratamiento a la hora de imponer la sanción.

4. Conclusiones y propuestas a las Administraciones Públicas.

En virtud de todo lo expuesto a lo largo del presente documento, podemos determinar que, para la contratación de servicios en la nube, deben tenerse en cuenta todos los riesgos potenciales inherentes a este tipo de servicios; las transmisiones de datos personales custodiadas por las Administraciones Públicas a terceros.

Para evitar, o minimizar al máximo estos riesgos, conociendo el panorama actual respecto a las transferencias de datos internacionales, en contraste con la industria de los proveedores de cloud computing, que se encuentran altamente concentrada en unos pocos actores en los Estados Unidos. El problema principal de realizar transferencias internacionales a Estados Unidos radica en que, no cumple el RGPD en el tratamiento de los datos que se transfieren, esto es debido a que las autoridades gubernamentales y centros de inteligencia pueden acceder sin limitación alguna y sin necesidad de autorización judicial a los datos transferidos, por lo que desde la UE, desde 2020 a raíz del famoso caso Schrems, Estados Unidos tiene la consideración de no seguro para transferir datos desde la UE al no ofrecer garantías suficientes para la seguridad de los datos.

Es por ello que, a la haora de evaluar los posibles adjudicatarios de licitaciones, las Administraciones Públicas deben valorar positivamente a los proveedores que cumplan RGPD respecto a las transferencias internacionales,evitando transferencias a territorios inseguros, se evita el riesgo. De este modo proponemos que se apoye a los proveedores de cloud computing otorgando mayor puntuación en las licitaciones, que los proveedores que estén situados en terceros países fuera de la Unión.

En definitiva, promover contratación en prestadores de servicios de cloud locales, situados en el Espacio Económico Europeo, trae consigo beneficios considerables a los Entes Públicos que buscan proveedores capaces de cumplir con los estándares de seguridad del tratamiento de los datos regulados en el artículo 32 del RGPD, que en caso de incumplimiento, la infracción se atribuye tanto al responsable (Administración Pública) como encargado del tratamiento (proveedor de servicios).

Igualmente, la contratación de proveedores comunitarios propicia una mejora en la competencia al desconcentrar el mercado de cloud computing en las grandes tecnológicas estadounidenses, impulsando así un ecosistema de innovación que configura una fuente de empleo y crecimiento de la economía en el Espacio Económico Europeo. De este modo proponemos que en las licitaciones se apoye a los proveedores de Cloud Computing europeos

otorgando mayor puntuación a los proveedores con equipamiento y domicilio social en la UE (no sujetos a la legislación de EEUU), respecto a los que estén situados en terceros países fuera de la Unión. Es de especial relevancia que los proveedores no se encuentren sometidos a la legislación estadounidense, es decir, que no sean empresas de este país, puesto que, a la luz del *Cloud Act* los proveedores americanos que operan en la Unión Europea, aunque tengan sus centros de datos en territorio europeo y cumplan las leyes europeas, en virtud de dicha normativa quedan sometidos a la ley estadounidense, debiendo proporcionar acceso a las autoridades de inteligencia estadounidenses a los datos que sean requeridos provenientes de la Unión Europea.

Desde julio de 2023, se ha introducido un nuevo marco normativo el "*Data Privacy Framework UE-EEUU"* (DPF) donde, para el acceso por parte de las autoridades estadounidenses a los datos europeos, **deben imperar razones de necesidad y proporcionalidad para la seguridad nacional que justifiquen tal acceso**, adicionalmente este nuevo marco instaura **mecanismos de supervisión por parte de las autoridades europeas** de las actividades que realicen los servicios de inteligencia estadounidenses para garantizar el cumplimiento de las nuevas limitaciones en sus actividades de vigilancia.

Este nuevo marco normativo, surge a partir de una Decisión de Adecuación por parte de la UE tras la firma por parte de EEUU de una Orden Ejecutiva sobre "*Enhancing Safeguards for United States Signals Intelligence Activities*", que introdujo nuevas salvaguardias vinculantes para abordar los puntos planteados por el Tribunal de Justicia de la Unión Europea en su decisión Schrems II de julio de 2020. Esta decisión de adecuación concluye que Estados Unidos garantiza un nivel adecuado de protección (en comparación con el de la UE) para los datos personales transferidos desde la UE a empresas estadounidenses que participan en el *Data Privacy Framework UE-EEUU*.

Un elemento esencial del marco jurídico estadounidense en el que se basa la decisión de adecuación es la Orden Ejecutiva sobre "*Enhancing Safeguards for United States Signals Intelligence Activities*", firmada por el Presidente Biden el 7 de octubre. Estos instrumentos se adoptaron para abordar las cuestiones planteadas por el Tribunal de Justicia en su sentencia Schrems II.

Para los europeos cuyos datos personales se transfieren a los EEUU, la Orden Ejecutiva prevé:

- Salvaguardias vinculantes que limiten el acceso a los datos por parte de las autoridades de inteligencia estadounidenses a lo que sea necesario y proporcionado para proteger la seguridad nacional.
- Mayor supervisión de las actividades de los servicios de inteligencia estadounidenses para garantizar el cumplimiento de las limitaciones a las actividades de vigilancia.

- El establecimiento de un mecanismo de reparación independiente e imparcial, que incluya un nuevo Tribunal de Revisión de Protección de Datos para investigar y resolver quejas relacionadas con el acceso a sus datos por parte de las autoridades de seguridad nacional de Estados Unidos.

En virtud de este nuevo marco, el gobierno de los Estados Unidos ha establecido un mecanismo de reparación de dos niveles, a través de una autoridad independiente y vinculante, para manejar y resolver quejas de cualquier individuo cuyos datos hayan sido transferidos del Espacio Económico Europeo a empresas en los EEUU sobre la recopilación y el uso de sus datos por parte de las agencias de inteligencia estadounidenses, donde **los interesados pueden presentar una reclamación ante su autoridad nacional de protección de datos**, lo que garantizará que la reclamación se transmita adecuadamente y que se proporcione a la persona cualquier información adicional relacionada con el procedimiento. **Las quejas serán transmitidas a los Estados Unidos por el Consejo Europeo de Protección de Datos.**

En primer lugar, las quejas serán investigadas por la figura del "Oficial de Protección de las Libertades Civiles" (CLPO) de la comunidad de inteligencia estadounidense responsable de garantizar el cumplimiento por parte de las agencias de inteligencia estadounidenses de la privacidad y los derechos fundamentales. A la fecha de la investigación, no se deduce que existan mecanismos aprobados y habilitados para el nombramiento de esta figura, lo que dificulta el ejercicio de derechos de los interesados.

En segundo lugar, los interesados tienen la posibilidad de apelar la decisión del Oficial de Protección de Libertades Civiles ante el recién creado Tribunal de Revisión de Protección de Datos (DPRC) El Tribunal está compuesto por miembros ajenos al gobierno de los EEUU, que son nombrados sobre la base de calificaciones específicas, sólo pueden ser destituidos por causa justificada (como una condena penal o ser considerados mental o físicamente no aptos para realizar sus tareas) y no pueden recibir instrucciones del gobierno. El DPRC tiene poderes para investigar reclamaciones de individuos de la UE, incluso para obtener información relevante de agencias estadounidenses. Del mismo modo, a la fecha de la investigación, no se han encontrado mecanismos que expongan el procedimiento o criterios para el nombramiento de este Tribunal.

Sin embargo, la aplicación del *Data Privacy Framework UE-EEUU* se supedita a la auto certificación anual de dicho marco por parte de las empresas estadounidenses, ante la autoridad estadounidense *The International Trade Administration (ITA)* adscrita al *U.S. Department of Commerce* (que también actúa como enlace con las autoridades de protección

de datos de la UE[16]). Las organizaciones podrán disfrutar de los beneficios del DPF una vez que la ITA coloque a la organización en el "*Data Privacy Framework List*[17]"

Los principios que rigen esta autocertificación se engloban en siete puntos principales:

1.- Aviso: Las organizaciones adheridas al DPF deben informar sobre su participación y proporcionar un enlace o la dirección web de la Lista del marco de privacidad de datos y proporcionar información sobre los datos que se recopilan, la finalidad con la que se recopilan, el derecho de los interesados de acceder a los datos…

También deberán informar las organizaciones adheridas sobre la existencia de un organismo independiente de resolución de disputas designado para atender quejas y brindar un recurso adecuado y gratuito al interesados, y si es: (1) un punto de contacto establecido por las Autoridades de Protección de Datos, (2) un proveedor alternativo de resolución de disputas con sede en la UE, o (3) un proveedor alternativo de resolución de disputas con sede en los Estados Unidos

Igualmente deberán informar acerca de la obligación de la organización de revelar información personal en respuesta a solicitudes legales de autoridades públicas, incluso para cumplir con requisitos de seguridad nacional o de aplicación de la ley.

2.- Elección: La organización debe ofrecer a las personas la opción de participar en si su información personal (i) se divulgará a un tercero o (ii) se utilizará de forma posterior para un propósito distinto del propósito para el cual fue originalmente recopilado. Se debe proporcionar a los individuos mecanismos claros, visibles y fácilmente disponibles para ejercer sus opciones. Para información sensible (datos médicos, ideología, origen racial…) se debe obtener el consentimiento expreso de los interesados.

3.- Responsabilidad por transferencias adicionales: se deberán transferir dichos datos sólo para fines limitados y específicos, asimismo, el tercero deberá proporcionar al menos el mismo nivel de protección de la privacidad que exigen los Principios del DPF.

4.- Seguridad: Las organizaciones que traten información personal deben tomar medidas razonables y apropiadas para protegerse contra la pérdida, mal uso y acceso no autorizado, divulgación, alteración y destrucción, teniendo debidamente en cuenta los riesgos involucrados en el procesamiento y la naturaleza de los datos personales.

16 https://www.dataprivacyframework.gov/s/article/European-DPA-Liaison-at-the-U-S-Department-of-Commerce-dpf

17 https://www.dataprivacyframework.gov/s/participant-search

5.- Integridad de los datos y limitación de finalidad: la información personal debe limitarse a la información que sea relevante para los fines del procesamiento. Una organización no puede procesar información personal de una manera que sea incompatible con los fines para los cuales ha sido recopilada o posteriormente autorizada por el individuo.

6.- Acceso: Las personas deben tener acceso a la información personal sobre ellas que posee una organización y poder corregir, modificar o eliminar esa información cuando sea inexacta o haya sido procesada en violación de los Principios del DPF. Este derecho de Acceso podrá negarse cuando la carga o el gasto de proporcionar acceso sea desproporcionado con los riesgos para la privacidad del interesado, o cuando se violarían los derechos de personas distintas del interesado.

7.- Recurso, ejecución y responsabilidad: Las organizaciones deben incluir:
(a) Mecanismos de recurso independientes, fácilmente disponibles mediante los cuales, las quejas y disputas de cada individuo se investigan y resuelven rápidamente sin costo para el individuo.
(b) Procedimientos de seguimiento para verificar que las declaraciones y afirmaciones que las organizaciones hacen sobre sus prácticas de privacidad son verdaderas y que las prácticas de privacidad se han implementado tal como se presentan.
(c) Obligaciones de remediar los problemas que surjan del incumplimiento de los Principios por parte de las organizaciones que anuncian su adhesión a ellos y las consecuencias para dichas organizaciones.

Sin embargo, el cumplimiento de estos Principios podrá limitarse en determinados casos:

(a) Para cumplir con una orden judicial o satisfacer requisitos de interés público, aplicación de la ley o seguridad nacional, incluso cuando los estatutos o regulaciones gubernamentales creen obligaciones contradictorias.
(b) Por obligación legal, orden judicial o regulación gubernamental que cree autorizaciones explícitas, siempre que, al ejercer dicha autorización, una organización pueda demostrar que su incumplimiento de los Principios se limita al grado necesario para satisfacer los intereses legítimos primordiales. promovido por dicha autorización.

Para más información del resto de Principios complementarios están disponibles en la siguiente Enlace:

https://www.dataprivacyframework.gov/s/article/I-OVERVIEW-dpf?tabset-35584=2

Se establece además, que **la ley de los EEUU será de aplicación en lo relativo a las cuestiones de interpretación y cumplimiento de los Principios y las políticas de**

privacidad relevantes por parte de las organizaciones que participan en el DPF, excepto cuando dichas organizaciones se hayan comprometido a cooperar con las autoridades de protección de datos de la UE[18]. Esta particularidad puede generar graves problemas respecto a la aplicación de los principios de proporcionalidad y necesidad para el acceso de los datos por las autoridades de inteligencia, donde los criterios de interpretación que pueden darse en virtud del RGPD no son obligatorios.

Es relevante destacar, que esta auto-certificación, no es obligatoria para las empresas, por lo que mientras no se adhieran a este nuevo marco regulatorio, será de aplicación el *Cloud Act.* Es decir, el *Cloud Act* no queda derogado con la introducción del *Data Privacy Framework UE-EEUU*, y solo se consideran suficientemente seguras para las transferencias internacionales aquellas empresas participantes en la certificación del nuevo marco de privacidad, característica muy relevante que no se menciona en los pliegos administrativos analizados.

Por lo expuesto, concluimos que, aunque el DPF logra mejoras respecto a las transferencias de datos provenientes de la UE, sigue existiendo el riesgo de incumplimiento por parte de las autoridades estadounidenses del *Data Privacy Framework UE-EEUU* debido a:
1.- Los juicios de proporcionalidad y necesidad que se puedan considerar aplicables, puesto que el DPF no requiere necesariamente aplicar los criterios de interpretación que establece el RGPD.
2.- No están definidos el funcionamiento ni el nombramiento tanto de la figura de Oficial de Protección de las Libertades Civiles como del Tribunal de Revisión de Protección de Datos.

Con la información disponible en las fuentes oficiales no identificamos que estén definidos los criterios para evaluar el cumplimiento por parte de las empresas americanas de la normativa de protección de datos europea (RGPD).

Por lo expuesto consideramos que a la fecha no resulta suficientemente seguro las transferencias internacionales de datos europeos a las empresas americanas, aunque tengan sede e infraestructura para el tratamiento de datos ubicados en Europa.

En Madrid, a 10 de octubre de 2023

[18] https://www.dataprivacyframework.gov/s/article/I-OVERVIEW-dpf?tabset-35584=2

Sor Arteaga[19]
PhD Doctora en Derecho. Abogada colegiada Nº 105.096 del ICAM
DPO. Especialista en Protección de Datos, Telecomunicaciones e IT

[19] **Sor Arteaga**, dispone de más de 15 años de experiencia en el asesoramiento y consultoría a operadores nacionales e internacionales en materia de derecho de las telecomunicaciones, incluyendo empresas importantes del sector. Es Doctora en Derecho- Estudios Europeos de la Universidad CEU San Pablo de Madrid, cuenta con Máster en Derecho de las Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información en la Universidad Carlos III de Madrid. Estudios Avanzados en Gobierno y Administración Pública en la Universidad Complutense de Madrid- Fundación Ortega y Gasset, Diploma de estudios avanzados en Derecho Constitucional. Es Personal docente del Máster Universitario en Derecho de las Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información de la Universidad Carlos III de Madrid, y en la Universidad de Nebrija. Es miembro del Grupo de Investigación en Gobierno, Administración y Políticas Públicas en España y Latinoamérica (GIGAPP), adicionalmente, ha sido investigadora de los Proyectos de investigación I+D "Protección de Datos, Transparencia, Seguridad y Mercado" (DER 2009-13.184) y "Protección de Datos y Aplicación Extraterritorial de las Normas. Reforma de la Directiva sobre Protección de Datos" de la Universidad CEU-San Pablo, Referencia DER 2012-35948 financiados por el Ministerio de Economía y Competitividad de España dirigido por D. José Luis Piñar Mañas (ex Director de la Agencia Española de Protección de Datos), y dispone de diversos artículos y publicaciones en el sector.