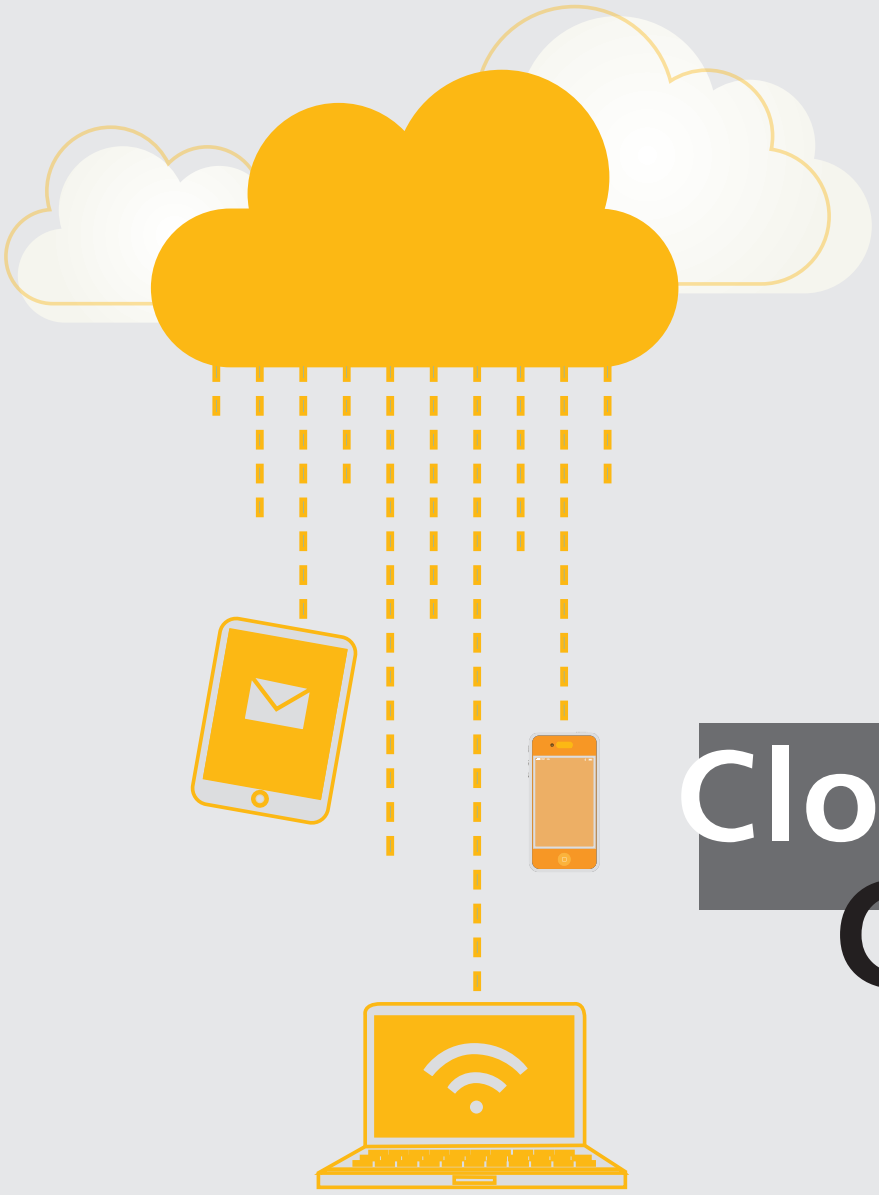
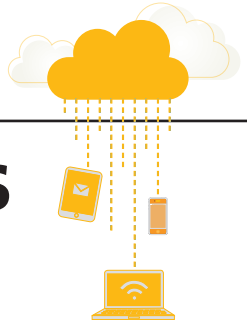
AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS



ORIENTACIONES para PRESTADORES de SERVICIOS de Cloud Computing



ORIENTACIONES para PRESTADORES de SERVICIOS de Cloud Computing

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

índice

4 INTRODUCCIÓN

5 LOS SUJETOS QUE INTERVIENEN EN LA CONTRATACIÓN DE SERVICIOS DE ‘CLOUD COMPUTING’ Y LA LEY APLICABLE

6 DILIGENCIA Y TRANSPARENCIA EN LA CONTRATACIÓN

7 GARANTÍAS QUE DEBEN INCORPORARSE AL CONTRATO

8 LAS TRANSFERENCIAS INTERNACIONALES DE DATOS

9 EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, SUPRESIÓN, LIMITACIÓN DEL TRATAMIENTO, PORTABILIDAD, OPOSICIÓN Y DECISIONES INDIVIDUALES AUTOMATIZADAS

9 LA CONTRATACIÓN CON ADMINISTRACIONES PÚBLICAS

ORIENTACIONES PARA PRESTADORES DE SERVICIOS DE 'CLOUD COMPUTING'

INTRODUCCIÓN

La Agenda Digital del Gobierno apuesta por potenciar las industrias de futuro con el fin de que España se mantenga en la vanguardia de la innovación y participe en las iniciativas que permitan detectar tendencias de futuro, generar empresas en dichos sectores e impulsar el talento y el emprendimiento.

En este sentido destaca como una línea específica de actuación la potenciación y uso del *cloud computing* como 'un mecanismo clave para garantizar la competitividad de nuestras empresas', especialmente las pymes, así como facilitar su utilización por parte de la Administración.

En este marco, no cabe olvidar que los servicios de *cloud computing* tienen implicaciones específicas para la protección de los datos personales de los que es responsable el cliente que contrata dichos servicios. Esas implicaciones exigen una valoración del mejor modo de incorporar las garantías contempladas en la normativa de protección de datos, modulándolas para adaptarlas a las características específicas de los mismos.

La Agencia Española de Protección de Datos ha asumido la iniciativa de elaborar unas orientaciones que faciliten, didácticamente, su cumplimiento.

Para ello ha elaborado dos documentos dirigidos, respectivamente, a los clientes que contraten servicios de *cloud computing* y a los proveedores que los prestan.

El primer documento, articulado como una guía práctica, es más extenso y detallado dado el mayor desconocimiento que pueden tener en esta materia los clientes, especialmente las pymes y los profesionales.

El presente documento, dirigido a los prestadores de estos servicios, es más sintético tratando de evitar reiteraciones con el anterior, pero ofreciendo información complementaria mediante remisiones a aquel.

Las orientaciones tienen como objetivo reiterar, especialmente a las grandes corporaciones que ofertan masivamente estos servicios y a quienes ofrecen contratos de adhesión a sus potenciales clientes, que deben adaptarse al régimen de garantías que la normativa de protección de datos personales atribuye a los ciudadanos.

Con ello, la Agencia pretende impulsar una política preventiva para el cumplimiento de la ley haciendo hincapié en que los clientes de servicios de *cloud computing* tengan en cuenta, a la hora de seleccionar a su proveedor, a aquellos cuya oferta minimice los riesgos de incumplimiento.

LOS SUJETOS QUE INTERVIENEN EN LA CONTRATACIÓN DE SERVICIOS DE 'CLOUD COMPUTING' Y LA LEY APLICABLE

La aplicación de la normativa de protección de datos a la oferta de servicio de *cloud computing* ha de tener como punto de partida la identificación de la posición jurídica que ocupan, respectivamente, el proveedor de dichos servicios y los clientes con los que contrata.

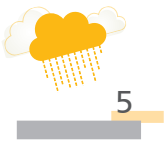
La citada normativa distingue dos sujetos distintos: el responsable del fichero o del tratamiento de los datos y el encargado del tratamiento.

El primero es la persona, profesional o entidad que decide sobre la finalidad, contenido y uso del tratamiento.

En consecuencia, el cliente que contrata servicios de *cloud computing,* al tomar decisiones sobre la contratación de dichos servicios, el mantenimiento o no de sus propios sistemas de información, la modalidad de *nube* y la tipología de servicios que contrata y la elección del proveedor en función de las condiciones ofrecidas, sigue manteniendo la condición de responsable del tratamiento de los datos sobre los que se aplicarán los citados servicios. Esta responsabilidad, al derivarse de la aplicación de la ley, no puede alterarse contractualmente.

Por su parte, el proveedor de servicios de *cloud computing* que implican el acceso a datos personales, aunque sea una gran corporación que se encuentra en una posición prevalente sobre sus clientes, será un prestador de servicios, es decir, un encargado del tratamiento en la terminología de la citada normativa.

Esta aproximación inicial sobre la posición jurídica que ocupan el cliente y el prestador de servicios tiene como consecuencia principal la determinación de la ley aplicable, que será la del cliente.



Por tanto, si los clientes/responsables del tratamiento de los datos personales tienen un establecimiento en la Unión Europea o si, sin estar establecidos en la Unión, tratan datos personales de interesados que residan en la misma para la oferta de bienes o servicios o para el control de su comportamiento, la relación jurídica con el prestador de servicios estará sometida al 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 (Reglamento general de protección de datos o RGPD) La determinación de la ley aplicable es, asimismo, una cuestión que no es disponible para las partes.

DILIGENCIA Y TRANSPARENCIA EN LA CONTRATACIÓN

El cliente que contrata aun prestador de servicios de cloud computing tiene una obligación legal de diligencia para, según el artículo 28.1 del RGPD, elegir "únicamente un encargado que ofrezca 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".

Este deber de diligencia se traducirá, dadas las características propias de estos servicios, en un abanico de requerimientos de información al proveedor de servicios dirigidos a conocer las garantías que ofrece para la protección de los datos personales de los que sigue siendo responsable.

Dicha información le resultará imprescindible para decidir sobre la modalidad de *nube* y el tipo de servicios que contrata y, específicamente, para discriminar cuál o cuáles le ofrecen garantías adecuadas y elegir entre ellos.

El cumplimiento de este deber de diligencia ha de tener como contrapartida por parte del prestador de servicios de cloud computing una correlativa diligencia a la hora de facilitar información, en particular sobre los mecanismos que garantizan el cumplimiento de las obligaciones derivadas de la normativa de protección de datos, para poder considerarlo como un proveedor transparente, como se establece en el art. 28.3 letra h): "pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable" así como en el párrafo final del mismo artículo ", el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros".

La transparencia es, por tanto, un principio esencial que debe presidir las relaciones entre las partes, especialmente en los casos en que el proveedor de servicios ocupa una posición preeminente sobre los clientes. Circunstancia que será habitual cuando estos últimos sean pymes, microempresas, profesionales o Administraciones públicas sin gran estructura orgánica.

A tal efecto, la Guía para clientes que contraten servicios de cloud computing incluye un abanico de preguntas sobre las garantías exigibles que han de ser atendidas por el proveedor que los comercializa a cuyo contenido se remite este documento (Guía disponible en www.aepd.es). En particular, el RGPD estable en el artículo 28.1.5 que "La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo."

Es por ello que la Agencia Española de Protección de datos valorará particularmente la diligencia y transparencia en la contratación de estos servicios.

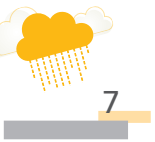
GARANTÍAS QUE DEBEN INCORPORARSE AL CONTRATO

La normativa de protección de datos personales exige en los casos de prestación de servicios la celebración de un contrato cuyo contenido permita acreditar la incorporación de las garantías exigidas por el artículo 28 del RGPD . Este artículo recoge en su apartado 3 un conjunto de cláusulas contractuales más amplio que el de la LOPD, por lo que es necesario proceder a la adaptación de los contratos.

En el caso de que intervengan terceras empresas subcontratadas para la prestación del servicio que se ofrece, es necesario adoptar garantías adicionales (que han sido ratificadas por la Sentencia del Tribunal Supremo de 15 de julio de 2010, F.D. Décimo).

Estas garantías se refieren a los siguientes aspectos:

- La identificación de los servicios y la empresa a subcontratar informando de ello al cliente (incluido el país en el que desarrolla sus servicios si están previstas transferencias internacionales de datos).
- Que el cliente pueda tomar decisiones como consecuencia de la intervención de subcontratistas.
- La celebración de un contrato entre el prestador de servicios de *cloud computing* y los subcontratistas con garantías equivalentes a las incluidas en el contrato con el cliente.



No obstante, dadas las características especificas de los servicios de *cloud computing,* las garantías exigibles pueden modularse para adaptarlas a los requisitos del RGPD (para conocer algunos ejemplos sobre esta cuestión puede accederse a la *Guía para clientes que contraten servicios de cloud computing*, disponible en www.aepd.es. Las soluciones que se recogen deben tomarse como meros ejemplos, pudiendo adoptarse otras soluciones que ofrezcan las mismas garantías).

Estas garantías también han de proporcionarlas aquellas compañías que actúan como *partners* de otros proveedores de *cloud computing*, en cualquiera de las figuras de *reseller*, agregadores de servicios de *cloud*, *cloud builders*, proveedores de aplicaciones, etc., y que proporcionan servicios contratando directamente con los clientes.

La portabilidad, es decir, la posibilidad efectiva de que los datos personales puedan ser devueltos al cliente o que éste pueda indicar que se transfieran a un nuevo proveedor de servicios que haya seleccionado, en el momento en que finalice la prestación del mismo, es una garantía que ha de tenerse especialmente en cuenta, independientemente del derecho a la portabilidad que reconoce el RGPD a las personas físicas.

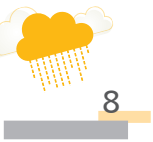
Por ello, el contrato debe incluir soluciones específicas para garantizar esa portabilidad, adaptadas a las distintas modalidades de *cloud* y al tipo de servicios que se ofrezcan.

Las garantías sobre la portabilidad en materia de protección de datos personales son independientes de las que se deriven del término de la prestación de servicios conforme al derecho privado, si bien las condiciones contractuales en este ámbito no deberán imposibilitar aquella.

LAS TRANSFERENCIAS INTERNACIONALES DE DATOS

La prestación de servicios de cloud computing implicará, en numerosas ocasiones, flujos transfronterizos de datos a terceros países que implican una transferencia internacional de datos. No tienen esta consideración los flujos de datos que se producen dentro del marco del Espacio Común Europeo (los Estados de la Unión Europea más Islandia, Noruega y Liechtenstein).

Cuando se produzcan transferencias internacionales de datos deben realizarse con garantías adecuadas. Especialmente importante, dadas las características propias de los servicios de *cloud computing*, es establecer mecanismos para permitir que las subcontrataciones que se realicen en este contexto de transferencias internacionales se gestionen con fluidez, asegurando al mismo tiempo que el cliente responsable tiene información suficiente sobre los subcontratistas, o potenciales subcontratistas, y mantiene la capacidad de tomar decisiones. (Para obtener más información puede consultar la *Guía para clientes que contraten servicios de cloud computing*)



EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, SUPRESIÓN, LIMITACIÓN DEL TRATAMIENTO, PORTABILIDAD, OPOSICIÓN Y DECISIONES INDIVIDUALES AUTOMATIZADAS

El cliente que contrate servicios de cloud computing, al seguir siendo el responsable del tratamiento de los datos personales, está obligado a facilitar el ejercicio de los derechos reconocidos en los artículos del 15 al 22 del RGPD a los interesados en los plazos legales.

Para ello es posible que precise de la colaboración del prestador de servicios de *cloud computing*.

Por tanto, el proveedor de estos servicios debe prever que pueda ser necesaria esta colaboración, proporcionar información al respecto y, cuando se solicite, hacerla efectiva diligentemente.

LA CONTRATACIÓN CON ADMINISTRACIONES PÚBLICAS

Si el prestador de servicios de *cloud computing* proyecta ofrecerlos a las Administraciones públicas ha de tener presente que están sujetas a obligaciones legales adicionales, por lo que deberá configurar sus servicios de forma que permitan su cumplimiento.

En particular debe reiterarse que el responsable tiene una obligación de diligencia específica para contratar a un encargado de tratamiento que cumpla con las garantías previstas en el RGPD, por lo que deberá facilitarse la información que resulte precisa.

En este sentido, cabe indicar que la 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, incluye en su Disposición Adicional Vigésima Quinta las garantías aplicables a la prestación de servicios que impliquen el tratamiento de datos personales, incluidos los supuestos de subcontratación.

Otras normas que se deben considerar es la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Asimismo, es necesario ofrecer servicios adaptados al Esquema Nacional de Seguridad y al Esquema Nacional de Interoperabilidad (Reales Decreto 3/2010 y 4/2010, de 8 de enero).

Finalmente, de existir la posibilidad de que, al realizarse transferencias internacionales de datos, autoridades de terceros países puedan requerir accesos a la información, ha de informarse sobre esta posibilidad y sobre las opciones que la Administración que contrate los servicios puede adoptar sobre ella (para mayor información sobre las especificidades en las Administraciones públicas, puede verse la *Guía para clientes que contraten servicios de cloud computing*, disponible en www.aepd.es).

Para concluir este documento, la Agencia Española de Protección de Datos recomienda a los prestadores de servicios de *cloud computing* tener en cuenta los siguientes puntos:

- Revisar sus contratos teniendo en cuenta los criterios recogidos en este documento.
- Adaptarlos para que los cumplan.
- Informar a sus clientes, si no los cumplen, de la necesidad de adoptar estas garantías.
- La responsabilidad por incumplimiento de la ley puede exigirse al cliente y también al prestador de servicios.

www.aepd.es