Grupo de Trabajo -Privacy Level Agreement

Esquema de Privacy Level Agreement (PLA) para la Venta de Servicios en la Nube en la Unión Europea

Febrero 2013- EN
Julio 2013- ES

El esquema PLA se ha desarrollado dentro de CSA, por un grupo de expertos integrado por representantes de proveedores de servicios en la nube, autoridades locales de protección de datos; y profesionales independientes de la seguridad y de la privacidad. El grupo de trabajo está co-presidido por Paolo Balboni y Francoise Gilbert, bajo la supervisión técnica de Daniele Catteddu. La traducción al castellano se ha desarrollado dentro del capítulo español de CSA-ES, por un grupo de expertos formado por Josep Bardallo, Fernando Campo, José Leandro Núñez, Ramón Miralles, Nathaly Rey, Antonio Sanz y Jordi Vilanova.

Contenidos

I. Objetivos

1. Los Privacy Level Agreement´s (PLA´s) están destinados a usarse como un apéndice de los Acuerdos de Servicios de Cloud Computing, para describir el nivel de protección de la privacidad que un Proveedor de Servicios de Cloud (PSC) adoptará. Mientras que los Acuerdos de Nivel de Servicio (por sus siglas en inglés SLA´s) son usados generalmente para proveer métricas y otro tipo de información acerca del rendimiento de los servicios, los PLA´s se usarán para dirigir las prácticas en relación con la privacidad y la protección de datos de carácter personal.[16]

2. En un PLA, el PSC debería definir claramente el nivel de privacidad y protección de datos que se compromete a mantener con respecto al tratamiento de los datos de carácter personal.[17]

3. La adopción de una estructura común o esquema de PLA a nivel mundial, puede constituir un poderoso estándar de la industria y una herramienta auto regulatoria y de armonización, capaz de mejorar la adhesión y el cumplimiento de las obligaciones de transparencia y responsabilidad en materia de protección de datos.[18]

4. Un PLA puede ofrecer una clara y efectiva herramienta de comunicación con los clientes y clientes potenciales de servicios de cloud, sobre el nivel de protección de datos ofrecido por el PSC, especialmente cuando existen movimientos transfronterizos de datos.[19]

---

[16] "Datos personales" o "datos": se entenderá como cualquier tipo de información referente a una persona identificable. Una persona identificable es aquella que puede ser identificada, directa o indirectamente, en particular por referencia a un número de identificación o uno o más factores específicos a su identidad física, psicológica, mental, económica, cultural o social. Artículo 2.a, Directiva 95/46/CE.

[17] "Tratamiento de datos o "tratamiento": se entenderá como cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;". Artículo 2.b, Directiva 95/46/CE.

[18] El PLA parece encajar perfectamente en la acción clave 2: "Términos y condiciones de contratación seguras y justas" de la Estrategia Europea de Cloud Computing- COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES. COM (2012) 529 final "La identificación y difusión de las mejores prácticas en materia de modelos de condiciones contractuales acelerará la aceptación de la computación en nube, al aumentar la confianza de los clientes potenciales. La adopción de medidas adecuadas sobre las cláusulas contractuales puede resultar útil asimismo en el ámbito crucial de la protección de datos." (…) "Elaborar con las partes interesadas, cláusulas contractuales tipo para los acuerdos de nivel de servicios de computación en nube aplicables a los contratos entre proveedores de servicios en la nube y usuarios profesionales, teniendo en cuenta el acervo de la UE en curso de elaboración en este ámbito..." p. 12.

[19] "Los proveedores de servicios en la nube que operan en la UE deberían brindar al cliente toda la información necesaria para evaluar correctamente los pros y contras de adoptar sus servicios. Seguridad, transparencia y seguridad jurídica para el cliente, deberían ser los factores clave de la oferta de los servicios en la nube". Opinión 05/2012 sobre Cloud Computing del Grupo de Trabajo del artículo 29 ("**A.29WP05/2012**"), p.2; "una precondición para la confianza en las disposiciones sobre servicios en la nube para el responsable del tratamiento (cliente de servicios Cloud) es realizar un ejercicio de evaluación

5. Por último, un PLA está destinado a proporcionar:

• A los clientes y clientes potenciales de servicios cloud, una herramienta para evaluar el compromiso del PSC en materia de privacidad y protección de datos personales (y como apoyo en el proceso de toma de decisión).

• A los PSC, una herramienta para la divulgación estructurada de sus prácticas en materia de privacidad y protección de datos personales.[20]

6. Este primer esquema de PLA proporciona una plantilla para efectuar declaraciones en materia de privacidad y protección de datos, respondiendo a las recomendaciones y orientaciones proporcionadas en 2012 por el Grupo de Trabajo del artículo 29; y de varias autoridades europeas de protección de datos, en diferentes documentos sobre contratos en la nube y el uso de servicios en la nube.

II. Suposiciones

Antes de suscribir un contrato para la provisión de servicios en la nube, un potencial cliente debería considerar la realización de una *due diligence* interna y de otra externa[21]:

- La *due diligence* interna debería ser utilizada para identificar las restricciones y limitaciones que podrían condicionar o impedir el potencial uso de servicios en la nube (p. ej. ¿es la nube una solución viable para el tipo de datos que la entidad quiere procesar?)
- La *due diligence* externa es una referencia para determinar si las propuestas de los PSC cumplen con las necesidades del cliente o cliente potencial. Podría ayudar a evaluar el nivel de protección de datos personales que un PSC garantizaría (p. ej. ¿garantiza el PSC el nivel de cumplimiento normativo que requiere la compañía contratante, bien en virtud de la normativa aplicable, o bien en virtud de requerimientos internos?).[22]

---

del riesgo, incluyendo la localización de los servidores donde los datos son procesados y la consideración de los riesgos y beneficios desde el punto de vista de protección de datos (…)" pág. 4.

[20] También de conformidad con A.29 WP05/2012.

[21] La Agencia Española de Protección de Datos (AEPD), publicó en mayo de 2013 la Guía para clientes que contraten servicios de 'Cloud Computing'. En su pág. 13, el documento contiene un apartado denominado "Estrategia para el cliente de servicios de computación en nube". http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf. Los objetivos de dicha estrategia se alinean con éste apartado.

[22] Para más información sobre este tema, ver la "Cloud Security Alliance Guidance" versión 3 en https://cloudsecurityalliance.org/research/security-guidance/ y su versión en castellano www.ismsforum.es/estudios/seguridadcloudv3

Due Diligence Interna

Como parte de su *due diligence* interna, una entidad que pretenda mover datos personales a la nube debería considerar, entre otros aspectos, los siguientes:

- Definir sus requisitos de seguridad, privacidad y cumplimiento normativo;
- Identificar qué datos, procesos o servicios quiere mover a la nube;
- Revisar su seguridad y políticas de privacidad interna, así como otras restricciones que puedan afectar al tratamiento de datos personales, tales como contratos pre-existentes, leyes y regulaciones aplicables, guías y mejores prácticas;
- Analizar y evaluar los riesgos de mover los datos a la nube;
- Identificar qué controles de seguridad (y certificaciones) son requeridos o útiles para alcanzar un nivel adecuado de protección de los datos personales de sus trabajadores o clientes mientras estos sean tratados en la nube;
- Definir responsabilidades y tareas para la implementación de los controles de seguridad (por ejemplo, entender qué controles de seguridad están bajo la responsabilidad de la cliente, y qué controles de seguridad deberían estar bajo la responsabilidad del PSC);
- Determinar que obligaciones tiene la entidad de monitorizar las actividades de su PSC (p. ej. ¿son requeridas visitas presenciales, o es suficiente una certificación o la garantía de una tercera parte?).

Due Diligence Externa

El cliente de servicios en la nube debería considerar realizar también una *due diligence* al PSC. Esta debería, entre otras cuestiones:

- Evaluar si el PSC cumple con los requisitos del cliente, respecto a privacidad y protección de datos usando el PLA;
- Comprobar si el PSC dispone de alguna certificación relevante o garantía basada en una evaluación o auditoría de un tercero independiente;
- Entender el cómo tener visibilidad, y monitorizar los controles de seguridad y prácticas implementadas por el PSC.

III. Notas Aclaratorias

Un PSC puede optar por usar diferentes PLA´s, dependiendo del tipo de servicio prestado, las diferentes ofertas, o las diferentes prácticas o mercados cubiertos. Por otra parte, un PLA puede apuntar o hacer referencias a otro documento para obtener más aclaraciones sobre un aspecto específico, el marco temporal, el alcance, la forma y el propósito del tratamiento de datos personales, así como el tipo de datos personales tratados –esta información debe ser recabada y consensuada con el cliente.[23]

Para evitar duplicidades, las referencias también se pueden hacer en un acuerdo de servicios marco, en un SLA, o en cualquier otro documento que contenga un contrato de servicios en la nube. Por ejemplo, los SLA´s típicamente incluyen información sobre seguridad de los datos. El uso estas de referencias cruzadas busca evitar la redundancia o duplicidad de las estipulaciones.

[23] A.29WP05/2012, Sección 3.4.2, p.13.

IV. Esquema del Privacy Level Agreement

1. Identidad del PSC (y de su Representante en la UE, si es el caso), su función, y la información de contacto del Delegado de Protección de Datos/ Data Privacy Officer (DPO) y del Delegado de Seguridad de la Información/ Information Security Officer (ISO)

Especificar:

- Denominación del PSC, dirección y lugar de establecimiento;
- Representante(s) local(es) (p.ej.: representante local en la UE);
- Cuál es la función asumida en materia de protección de datos con respecto a los tratamientos relevantes (p.ej.: responsable, co- responsable, encargado o sub-encargado);[24]
- Datos de contacto del DPO, si no existiera un DPO, los datos de contacto de la persona a cargo de los asuntos de privacidad que atenderá las solicitudes del cliente;
- Datos de contacto del ISO, si no existiera un ISO, los datos de contacto de la persona competente en materia de seguridad que atenderá las solicitudes del cliente.

[24] A.29WP05/2012 ha sido escrita teniendo en cuenta la situación en la que el cliente es un responsable y el PSC un encargado del tratamiento, consulte la Sección 1, página 4 y la Sección 3.4. En nuestra opinión, las funciones respectivas deben ser evaluadas cuidadosamente caso por caso, como también se ha confirmado por la Oficina del Comisionado de Información, en su Guía sobre el uso de la computación en nube ("ICO Guidance"), p. 7. A este respecto, véase el Sopot Memorándum, aprobado por el Grupo de Trabajo Internacional de Berlín sobre la protección de datos en Telecomunicaciones en abril de 2012 ("Sopot Memorandum") p.8 "Uno de los principios de protección de datos comúnmente reconocido es que el encargado del tratamiento no debe tratar datos personales más allá de las instrucciones explícitas del responsable. Para el Cloud Computing, esto implica que un proveedor de servicios en la nube no puede unilateralmente tomar una decisión o hacer ajustes en el tratamiento para transmitir más o menos automáticamente datos a centros de proceso desconocidos. Esto es así aunque el proveedor justifique dicha transferencia como una reducción de los costes operativos, la gestión de picos de cargas (desbordamiento), balanceo de carga, copia de la copia de seguridad, etc. Tampoco puede los datos personales para sus propias finalidades.";
A.29WP05/2012 p.23 "El borrador de propuesta aclara que un encargado del tratamiento que incumple las instrucciones del responsable, se califica como un responsable del tratamiento y está sujeto a las normas específicas de responsable conjunto "; recomendaciones de la CNIL para las empresas que planifican usar Servicios de Computación en la Nube "(recomendaciones de la CNIL ") páginas 5-6" Cuando un cliente utiliza un proveedor de servicios, en general se acepta que el primero es el responsable del fichero y el último es el encargado del tratamiento. Sin embargo, la CNIL considera que, en algunos casos de PaaS pública y SaaS, los clientes, aunque responsables de la elección de sus proveedores de servicios, no pueden realmente darles instrucciones y no están en condiciones de controlar la eficacia de la seguridad y las garantías de confidencialidad propuestas por los proveedores de servicios. Esta ausencia de instrucciones y de posibilidades de control se debe sobre todo a las ofertas estándar que no pueden ser modificados por los clientes, y para los contratos tipo que no les dan ninguna posibilidad de negociación. En tales situaciones, el proveedor de servicios podría, en principio, considerarse como responsable conjunto de conformidad con la definición de "responsable del tratamiento" contenida en el artículo 2 de la Directiva 95/46/CE, ya que contribuye a la definición de los objetivos y los medios para el tratamiento de datos personales. En los casos en los que hay responsables conjuntos, las responsabilidades de cada parte deben ser claramente definidas. "Siguiendo las indicaciones de la Autoridad de Protección de Datos italiana, el CSP es un encargado (del tratamiento), Cloud Computing: il Vademecum del Garante, pp.14-15. Véase también ICO Guide, pp 7-9 sobre las funciones de privacidad en los diferentes modelos de implementación de servicios en la nube. Por su parte, la Agencia Española de Protección de Datos considera el proveedor de servicios de Cloud Computing es un encargado de tratamiento, y que sólo si trata datos para fines propios puede ser considerado Responsable. En este sentido, veáse la Guía para clientes que contraten servicios de 'cloud computing'. Páginas 13-14.

2. Categorías de datos personales que el cliente tiene prohibido transmitir, o tratar en la nube
Especificar, si es el caso, qué categorías de datos personales tiene el cliente prohibido transmitir o tratar en la nube (por ejemplo, los datos relacionados con la salud).

3. Formas en las que los datos serán tratados
Si el PSC es un encargado del tratamiento, se debe incluir información detallada sobre el alcance y las modalidades en las que el cliente responsable del tratamiento poder dar instrucciones al PSC encargado del tratamiento.[25]

En su caso, diferenciar entre las actividades llevadas a cabo en nombre del cliente para proporcionar el (los) servicio (s) acordado (s) en la nube (por ejemplo, el almacenamiento de datos), las actividades llevadas a cabo a petición del cliente (por ejemplo, la preparación o producción de informes), y las llevadas a cabo por iniciativa del PSC (por ejemplo, copias de seguridad, recuperación ante desastres, monitorización del fraude).

Especificar cómo se informará al cliente de servicios en la nube sobre los cambios pertinentes en relación con el (los) servicio (s) acordado (s), tales como la implementación de funciones adicionales[26]

3.a - Ubicación de los datos personales
Especificar la (s) ubicación (es) de todos los centros de datos donde pueden ser tratados los datos personales,[27] y, en particular, dónde y cómo se podrán almacenar, duplicar en espejo, respaldar, y recuperar.

[25] A.29WP05/2012, Sección 3.4.2, p.12. "El acuerdo debe indicar explícitamente que el proveedor de servicios en la nube no puede utilizar los datos del responsable para su propias finalidades", Sopot Memorandum, p. 4. Véase también la ICO Guidance, p.12: "La autoridad de protección de datos requiere para el tratamiento de los datos tener un contrato por escrito (Apéndice 1, parte II párrafo 12 (a) (ii)) con el encargado del tratamiento)de datos requiere que el "encargado (del tratamiento) de datos sólo puede actuar con las instrucciones del responsable del tratamiento" y "el encargado del tratamiento deberá cumplir con las obligaciones de seguridad equivalentes a las impuestas en el tratamiento de los datos en sí". La existencia de un contrato escrito debe significar que el proveedor de servicios en la nube no podrá cambiar los términos de las operaciones (condiciones) de tratamiento de datos durante el período de vigencia del contrato sin el conocimiento y consentimiento del cliente de (servicios) en la nube. Los clientes (de servicios) en la Nube deben tener cuidado si un proveedor de servicios en la nube ofrece un "*lo tomas o lo dejas*", un conjunto de términos y condiciones sin la oportunidad de negociación. Estos contratos no permitirían que el cliente (de servicios) en la nube mantuviera (tuviera) un control suficiente sobre los datos con el fin de cumplir con las obligaciones de protección de datos. Por lo tanto, los clientes de servicios en la nube deben revisar los términos de servicio que un proveedor de (servicios) en la nube puede ofrecer para garantizar que se abordan adecuadamente los riesgos descritos en esta guía. "y p. 17: "El cliente (de servicios) en la nube debe asegurarse de que el proveedor de servicios en la nube sólo trata los datos personales para los fines previstos. El tratamiento para cualquier otro fin adicional podría romper el primer principio de la protección de datos. Este podría ser el caso si el proveedor (de servicios) en la nube decide utilizar los datos para sus propios fines. Los acuerdos contractuales deben evitarlo. "

[26] A.29WP05/2012, Sección 3.4.2, p.13. Véase también la sección 'legal' de la lista de verificación de la ICO Guidance, p. 22: "¿Cómo comunicará el proveedor de (servicios en) la nube los cambios en el servicio en la nube que puedan afectar a su contrato?"

[27] A.29WP05/2012, Sección 3.4.1.1, página 11 y la Sección 3.4.2, p.13. Ver también el principio de "transparencia de ubicación" "Sopot Memorandum ", p. 4 y las recomendaciones de la CNIL p.14. Véase también la sección 'legal' de la lista de verificación de la ICO Guidance, p. 22: "¿En qué países tratará los datos su proveedor de servicios en la nube y de que información dispone sobre las garantías locales en dichas localizaciones? ¿Puede garantizar que los derechos y las libertades de los interesados están protegidos? Usted debe preguntar al proveedor de servicios en la nube sobre las circunstancias en que sus datos podrán ser transferidos a otros países. ¿Puede su proveedor de servicios en la nube limitar la cesión de sus datos a los países que se consideren apropiados?

3.b - Subcontratistas

Identificar los subcontratistas y sub-encargados que participan en el tratamiento de datos, la cadena de responsabilidades, y el enfoque utilizado para garantizar que se cumplen los requerimientos de protección de datos.[28]

Identificar los procedimientos utilizados para informar al cliente de los cambios previstos en relación con la inclusión o sustitución de los subcontratistas o sub-encargados, manteniendo en todo momento los clientes responsables del tratamiento la posibilidad de oponerse a estos cambios, o de dar por terminado el contrato.[29]

3.c - Instalación de software en el sistema del cliente de servicios en la nube

Indicar si la prestación del servicio requiere de la instalación de software en el sistema del cliente (p. ej. plug-ins del navegador) y sus implicaciones desde una perspectiva de protección de datos y seguridad.[30]

4. Transferencia de datos

Indicar si los datos pueden ser transferidos, copiados y /o recuperados de forma transfronteriza, en el curso normal de las operaciones o ante una emergencia. Si dicha transferencia está restringida por las leyes aplicables, identificar el fundamento jurídico en el que se sustenta dicha transferencia (incluyendo transferencias sucesivas a través de varios niveles de subcontratistas).[31]

Indique si los datos se han de trasladar fuera del Espacio Económico Europeo. Si dicha transferencia tiene lugar, identificar en qué fundamento jurídico se sustenta: p. ej. Decisión de adecuación, clausulas tipo,[32] (Safe Harbor[33]) o Binding Corporate Rule´s (BCR´s).[34]

---

[28] Véase el concepto de "servicios por niveles" de “ICO Guidance", pp 6-8).

[29] A.29WP05/2012, Sección 3.3.2, p.10. "También debe ser clara obligación del proveedor de servicios en la nube de identificar a los encargados de los subcontratistas (por ejemplo, en un registro digital público)." A.29WP05/2012, Sección 3.4.2, p.13. Véase también la Sección 3.4.1.1 A.29WP05/2012 pp.10-11, ICO guidelines, p.11 y en el artículo 10 de la Directiva 95/46/CE.

[30] A.29WP05/2012, Sección 3.4.1.1, p.11.

[31] Véase ICO Guidance p.18.

[32] Veáse A29WP05/2012, Sección 3.5.3, p.18.

[33] "La comprobación del nivel adecuado, incluido los acuerdos de Puerto Seguro, están limitadas en el ámbito geográfico, y por lo tanto no se cubren todas las transferencias dentro de la nube. Las transferencias a las entidades estadounidenses adheridas a los principios de Puerto Seguro pueden llevarse a cabo legalmente de acuerdo a la legislación comunitaria, ya que las organizaciones beneficiarias se consideran que proporcionan un nivel adecuado de protección de los datos transferidos. Sin embargo, en opinión del Grupo de Trabajo, la simple auto-certificación de Puerto Seguro no puede considerarse suficiente en ausencia de adecuada aplicación de los principios de protección de datos en el entorno de la nube. Además, el artículo 17 de la Directiva de la UE, requiere que se firme un contrato entre el encargado del tratamiento y el Responsable para los fines del tratamiento, tal como se confirma en la pregunta 10 de los documentos del Marco de Trabajo de Puerto Seguro entre la UE y Estados Unidos.
Este contrato no está sujeto a la autorización previa de las autoridades de control europeas. Dicho contrato especifica el tratamiento a realizar y las medidas necesarias para garantizar que los datos se mantienen seguros. Diferentes legislaciones nacionales y las autoridades de protección de datos pueden imponer requisitos adicionales. El Grupo de Trabajo considera que las empresas que exporten datos no deben simplemente confiar en la declaración del importador de datos alegando que cuenta con la certificación Safe Harbor. Por el contrario, respecto de los datos exportados la empresa debe obtener evidencia de la existencia de la auto-certificación de Puerto Seguro y solicitar pruebas que demuestren que sus principios son respetados.
Esto es especialmente importante por lo que se refiere a la información proporcionada a los interesados afectados por el tratamiento de datos. El Grupo de Trabajo también considera que el cliente debe comprobar si los contratos tipo elaborados por los proveedores cumplen los requisitos nacionales sobre tratamiento de datos contractual. La legislación nacional puede exigir que el sub-tratamiento se defina en el contrato, lo que incluye datos sobre los lugares y otros relativos a los subencargados del tratamiento, así como la trazabilidad de los datos. Normalmente, los proveedores no ofrecen al cliente tal información –su compromiso con el puerto seguro no puede sustituir la falta de las garantías anteriormente mencionadas, cuando así lo exija la legislación nacional. En tal caso, se anima al exportador a que utilice otros instrumentos jurídicos disponibles, como cláusulas contractuales tipo o normas corporativas vinculantes/ oBinding Corporate Rule´s (BCR´s) . Por último, el Grupo de Trabajo considera que los principios de puerto seguro por sí solos

Medidas de seguridad

Especificar las medidas técnicas, físicas y organizativas implementadas para proteger los datos personales contra la destrucción, accidental o ilícita, y la pérdida accidental; alteración, uso, modificación, difusión o acceso no autorizados; y contra toda forma ilícita de tratamiento.

Describir las medidas técnicas, físicas y organizativas concretas que aseguren:[35]

- Disponibilidad:[36] describir los procesos y medidas implementadas para gestionar el riesgo de interrupción y prevenir, detectar y reaccionar ante incidentes, por ejemplo, copias de seguridad de los enlaces de Internet, almacenamiento redundante y mecanismos efectivos de creación y recuperación de copias de seguridad;[37]

- Integridad:[38] describir cómo asegura el proveedor de servicios la integridad (por ejemplo, detectando alteraciones en los datos mediante mecanismos criptográficos, tales como códigos de autenticación de mensajes o firmas);[39]

- Confidencialidad:[40] describir cómo asegura el proveedor de servicios la confidencialidad, desde un punto de vista técnico (por ejemplo, mediante el cifrado de los datos "en tránsito" y "en reposo",[25]

---

pueden no garantizar al exportador de datos los medios necesarios para asegurar que el proveedor ha aplicado las medidas de seguridad apropiadas en los Estados Unidos, según pueden requerir las legislaciones nacionales sobre la base de la Directiva 95/46/CE. En términos de seguridad de los datos, la computación en nube plantea varios riesgos de seguridad específicos de la nube, tales como perdidas de gobernanza, borrado inseguro o incompleto, evidencias de auditoria insuficientes o fallos de aislamiento de datos, que no son tenidos suficientemente en cuenta por los actuales principios de puerto seguro sobre la seguridad de los datos. Así pues, podrán establecerse garantías adicionales para la seguridad de los datos, por ejemplo mediante la incorporación de conocimientos y recursos de terceros que sean capaces de evaluar la adecuación de los proveedores mediante distintos sistemas de auditoria, normalización y certificación. Por estos motivos, podría ser aconsejable complementar el compromiso del importador de datos con el puerto seguro con salvaguardias adicionales que tengan en cuenta la naturaleza especifica de la nube". A29WP05/2012, apartado 3.5.1, pág. 18.

34 A29WP05/2012, apartado 3.5.4, p.19.

35 A29WP05/2012, apartado 3.5.4, p.13. Ver también ICO Guidance, págs 13-14.

36 Véase el apartado 'Disponibilidad' de la lista de verificación de la ICO Guidance, pág. 22: "¿Tiene el proveedor de (servicios en la) nube capacidad suficiente para hacer frente a una alta demanda de un pequeño número de otros clientes de (servicios en la) nube? ¿Cómo pueden afectar las acciones de otros clientes de (servicios en la) nube o de sus usuarios de (servicios en la) nube a la calidad de su servicio? ¿Puede garantizar que tendrá la posibilidad de acceder a los datos o a los servicios en el momento en que los necesite? ¿Cómo sufragará los costes de hardware y de conexión de los usuarios de (servicios en la) nube cuando estén fuera de la oficina? Si se produce una caída importante del proveedor de (servicios en la) nube, ¿cómo afectaría esto a su negocio?".

37 A.29WP05/2012, apartado 3.4.3.1, pág. 14.

38 Véase el apartado "Integridad" de la lista de verificación de la ICO Guidance, pág. 22: "¿Qué registros de auditoría se han implementado, a efectos de que se pueda supervisar quién accede a qué datos? Asegúrese de que el proveedor de (servicios en la) nube le permite obtener una copia de sus datos, en un formato utilizable, cuando así se lo solicite. ¿Cuánto tardaría el proveedor de (servicios en la) nube en recuperar sus datos (sin alteraciones) de una copia de seguridad en caso de que sufra una pérdida de datos importante?".

39 A.29WP05/2012, apartado 3.4.3.2, pág. 15. Véase también la ICO Guidance, pág. 22: "Asegúrese de que el proveedor de (servicios en la) nube le permite obtener una copia de sus datos, en un formato utilizable, cuando así se lo solicite".

40 Véase el apartado "Confidencialidad" de la lista de verificación de la ICO Guidance, pág. 22: "¿Puede su prestador de (servicios en la) nube facilitarte un análisis de seguridad adecuado, realizado por un tercero? ¿Cumple con los códigos de conducta del sector correspondiente, o con otros estándares de calidad? ¿Cuánto tardaría el proveedor de (servicios en la) nube en reaccionar si se detecta una vulnerabilidad de seguridad en su producto? ¿Cuáles son los plazos y costes por la creación, suspensión y borrado de cuentas? ¿Se cifran las comunicaciones en tránsito? ¿Es apropiado cifrar sus datos en reposo? ¿Qué gestor de claves se ha implementado? ¿Cuáles son los plazos de borrado y conservación de datos? ¿Incluyen la destrucción de los datos al final de su vida útil? El prestador de (servicios en la) nube, ¿procederá al borrado seguro de todos sus datos si usted decide abandonar la nube en el futuro? Entérese si sus datos, o los datos de sus usuarios, serán compartidos con terceros o compartidos a través de otros servicios que el prestador de (servicios en la) nube pueda ofrecer.

mecanismos de autorización y autenticación fuertes[26]) y desde un punto de vista contractual, mediante acuerdos o cláusulas de confidencialidad, y políticas empresariales vinculantes tanto para el proveedor de servicios o sus empleados (a tiempo completo o parcial, o contratados) como para sus subcontratistas (en su caso) que puedan acceder a los datos, para asegurar que sólo las personas autorizadas tienen acceso a los datos;[27]

- Transparencia: describir qué medidas técnicas, físicas y organizativas ha implementado el proveedor de servicios para apoyar la transparencia y permitir su revisión por los clientes (véanse, por ejemplo, los apartados 6 y 7);[28]

- Aislamiento (limitación de la finalidad): describir cómo presta aislamiento el proveedor (por ejemplo, la adecuada gobernanza de los derechos y roles de acceso los datos personales (revisados periódicamente), gestión de accesos basada en el principio del mínimo privilegio, mejora de los hipervisores y la correcta gestión de los recursos compartidos si se utilizan máquinas virtuales para compartir recursos físicos entre diferentes clientes);[29]

- Capacidad de intervención: describir cómo permite el proveedor a los interesados ejercitar sus derechos de acceso, rectificación, cancelación, bloqueo y oposición; de cara a demostrar la ausencia de obstáculos técnicos y organizativos en relación con dichas obligaciones, incluyendo aquellos casos en que los datos sean tratados posteriormente por subcontratistas;[30]

- Portabilidad: véase el apartado 9;

- Responsabilidad: véase el apartado 11.

---

25 Téngase en cuenta que "El cifrado de datos personales deberá utilizarse en todos los casos «en tránsito» y, cuando esté disponible, para los datos «en reposo» (…) Las comunicaciones entre el proveedor y el cliente, así como entre los centros de datos, deberán estar cifradas.". A.29WP05/2012, apartado 3.4.3.3, pág. 15. Véase también la ICO Guidance, págs. 14-15.

26 A.29WP05/2012, apartado 3.4.3.3, pág. 15.

27 A.29WP05/2012, apartado 3.4.2, pág. 13 y apartado 3.4.3.3, pág. 15. Véase también la ICO Guidance, pág. 17.

28 A.29WP05/2012, apartado 3.4.3.4, pág. 15. Asimismo, "La transparencia es un factor clave de cara a un tratamiento equitativo y legítimo de los datos personales. La Directiva 95/46/CE obliga al cliente a proporcionar al interesado cuyos datos se recaben información sobre su identidad y la finalidad del tratamiento. El cliente deberá facilitar también información adicional tal como la relativa a los destinatarios o categorías de destinatarios de los datos, que pueden incluir también los encargados del tratamiento y subencargados, en la medida en que dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado (artículo 10 de la Directiva).

La transparencia debe garantizarse también en la relación entre el cliente, el proveedor y los subcontratistas (en su caso). El cliente solo es capaz de evaluar la legalidad del tratamiento de datos personales en la nube si el proveedor le informa sobre todas las cuestiones pertinentes. Un responsable del tratamiento que contrate a un proveedor deberá comprobar cuidadosamente las condiciones de esté y evaluarlas desde el punto de vista de la protección de datos.

La transparencia en la nube supone que es necesario que el cliente tenga conocimiento de todos los subcontratistas que contribuyan a la prestación de los respectivos servicios en nube, así como de la localización de todos los centros donde puedan tratarse los datos personales.

Si la prestación del servicio requiere la instalación de programas informáticos en los sistemas del cliente (por ejemplo, plug-ins de navegador), el proveedor, a modo de buena práctica, deberá informar al cliente sobre esta circunstancia y, en particular, sobre sus implicaciones desde el punto de vista de la protección y la seguridad de los datos. E inversamente, el cliente deberá plantear esta cuestión con carácter previo, si no es abordada de manera suficiente por el proveedor." A.29WP05/2012, apartado 3.4.1.1, págs. 10-11.

29 A.29WP05/2012, apartado 3.4.3.5, pág. 16. Véase también la ICO Guidance pág. 20.

30 Téngase en cuenta que el prestador está obligado, en la práctica, a ayudar al cliente a la hora de facilitar el ejercicio de derechos por los interesados, y a asegurar que lo mismo ocurre en sus relaciones con cualquier subcontratista. A.29WP05/2012, apartado 3.4.3.5, pág. 16. Véase también la ICO Guidance, pág. 21.

Especificar qué marcos de control de seguridad se han implementado (por ejemplo, ISO/IEC 27002, CSA CMM, ENISA, Information Assurance Framework, etc.) y qué controles específicos se han aplicado.

6. Supervisión

Indicar si el cliente tiene la opción de monitorizar y/o auditar, en aras a asegurarse de que se cumplen con carácter permanente las medidas apropiadas de seguridad descritas en el PLA. Si tal supervisión es posible, especifíquese como (por ejemplo, mediante informes, auditorías).[31]

Especificar los controles que serán facilitados al cliente, así como los registros y auditorías de las correspondientes operaciones de tratamiento llevadas a cabo por el proveedor de servicios o sus subcontratistas.[32]

7. Auditorías de terceros

Especificar si se facilitan al cliente informes de auditoría realizados por terceros independientes, y en qué medida, así como su ámbito de aplicación, la frecuencia con la que dichos informes se actualizan y si se entrega al cliente el informe completo o un resumen del mismo.

Especificar si el auditor de la tercera parte confiable puede ser elegido por el cliente o por ambas partes, y quién pagará el coste de la auditoría.

8. Notificación de una violación de los datos personales

Una violación de los datos de carácter personal implica un fallo de seguridad que conduce a la pérdida, destrucción, alteración, revelación no autorizada o acceso, de forma accidental o ilegal, de datos de carácter personal transmitidos, almacenados o procesados de cualquier forma en conexión con la provisión de un servicio por parte de un PSC.

Especificar si y cómo se informará al cliente de las violaciones de datos de carácter personal y de seguridad que afecten a los datos procesados por el PSC y/o sus subcontratas, y dentro de qué marco temporal.[41]

9. Portabilidad de datos, migración, y ayuda en la transferencia de vuelta

31 Véase A.29WP05/2012, apartado 3.4.2, pág. 13. Véase también la ICO Guideline, págs. 13-14.
32 Véase A.29WP05/2012, apartado 3.4.1.2, pág.11.
41 Ver A.29WP05/2012, Sección 3.4.3.6, Pág.16.

Especificar los formatos, la preservación de relaciones lógicas y cualquier coste asociado con la portabilidad de datos, aplicaciones y servicios.[42]

Describir si, cómo y a qué coste el PSC ayudará a los clientes en una posible migración de los datos a otro proveedor o de vuelta a un entorno TI propio.[43]

10. Retención de datos, restablecimiento y borrado

Describir las políticas de retención de datos del PSC y las condiciones para devolver los datos de carácter personal y su destrucción una vez el servicio ha finalizado.

10.a - Política de retención de datos

Indicar durante cuánto tiempo se retendrán o podrán ser retenidos los datos de carácter personal.[44]

10.b - Borrado de datos

Indicar los métodos disponibles o empleados para borrar los datos, y si los datos pueden ser retenidos después de que el cliente haya borrado (o solicitado su borrado), o después de la finalización del contrato. Indicar en cada caso el periodo durante el cual el PSC retendrá los datos.

10.c – Retención de datos para el cumplimiento de requisitos legales

Describir cómo el PSC cumple con los requisitos legales relativos a la retención de datos que se aplican tanto al PSC como al cliente.

Indicar si y cómo el cliente puede solicitar al PSC que cumpla con normativas y leyes sectoriales específicas.[45]

---

42 Ver la guía del ICO, Pág. 22: "Asegurarse de que el proveedor Cloud te permite conseguir una copia de tus datos, bajo petición, en un formato usable".

43 Ver A.29WP05/2012, Sección 3.4.3.6, Pág.16.

44 Tener en cuenta que "Los datos de carácter personal deben de ser borrados (o anonimizados) tan pronto como ya no sea necesaria su retención". A.29WP05/2012, Sección 3.4.1, pag.10 y "si los datos no pueden ser borrados debido a normativas legales de retención (p.ej, normativa fiscal), el acceso a estos datos de carácter personal debería de ser bloqueado". Sección 3.4.1.3, Pág. 11 y "Dado que los datos de carácter personal pueden ser mantenidos de forma redundante en diferentes servidores y localizaciones distintas, debe de garantizarse que cada instancia de los mismos es borrada de forma irrecuperable (p.ej, versiones previas, temporales o incluso fragmentos de ficheros deberían ser borrados)". Ver también el Art.6 de la Directiva 95/46/CE. Ver también A.29WP05/2012, Sección 3.4.2, Pág.13.

45 Ver la guía ICO, Pág 16-17.

11. Responsabilidad

Describir qué políticas y procedimientos ha desplegado el PSC para garantizar y demostrar el cumplimiento legal, tanto por su parte, como por la de sus subcontratistas y socios de negocios, incluyendo la adopción de políticas internas y mecanismos que garanticen dicho cumplimiento legal (por ej. manteniendo documentación de todas las operaciones de procesado bajo su responsabilidad, y proporcionando una monitorización fiable y mecanismos de *log* exhaustivos).[46]

Identificar los certificados[47] de auditoría relevantes de terceras partes obtenidos por el PSC, su fecha y su alcance.[48]

12. Cooperación

Especificar cómo cooperará el PSC con el cliente Cloud para garantizar el cumplimiento legal de las disposiciones de protección de datos aplicables: por ej, para permitir que el cliente garantice el ejercicio de los derechos de sus interesados (acceso, rectificación, cancelación, bloqueo y oposición)[49]. [Ver también la Sección 5: Capacidad de intervención].

Describir cómo el PSC hará disponible al cliente y a las autoridades supervisoras la información necesaria para demostrar el cumplimiento legal.

13. Acceso de las autoridades competentes

---

46 Por favor, también tenga en cuenta que el CSP puede tener la obligación general de ofrecer garantías de que su organización interna y sus procedimientos de procesado de datos (y los de sus subcontratas, si los hubiere) cumplen con las leyes y estándares nacionales e internacionales aplicables, como se indica en A.29WP05/2012, Sección 3.4.2 Pág.14. Ver también el Artículo 17(2) de la Directiva 95/46/EC y A.29WP05/2012, Sección 3.4.3 Pág.14 and Sección 3.4.4.7. Ver también las recomendaciones del CNIL, Pág 12 "a) Cumplimiento de los principios de Francia acerca de la protección de datos de carácter personal [El modelo siguiente puede ser empleado cuando el proveedor de servicio es un procesador de datos] Las Partes comenzarán a recopilar y procesar todos los datos de carácter personal en cumplimiento de todas las regulaciones vigentes aplicables al procesado de estos datos, y en particular con la Ley 79-17 del 6 de Enero de 1978 y sus enmiendas. De acuerdo con esta ley, el Cliente es el controlador de los datos para el Procesado llevado a cabo según el Contrato [El modelo siguiente puede ser empleado cuando el proveedor de servicio es un controlador conjunto de datos] Las Partes comenzarán a recopilar y procesar todos los datos de carácter personal en cumplimiento de todas las regulaciones vigentes aplicables al procesado de estos datos, y en particular con la Ley 79-17 del 6 de Enero de 1978 y sus enmiendas. De acuerdo con esta ley, las Partes son controladoras conjuntas de los datos para el Procesado llevado a cabo según el Contrato".

47 Ej, Certificaciones ISO 27001, CSA STAR o SOC 2.

48 "Verificación o certificación independiente por parte de una tercera parte confiable puede ser una forma creíble a través de la que los proveedores Cloud demuestren su cumplimiento legal con sus obligaciones como se especifican en esta Opinión. Dicha certificación debería indicar, como mínimo, que los controles de protección de datos han sido sometidos a una auditoria o revisión contra un estándar reconocido, cumpliendo con los requisitos especificados por esta Opinión por una tercera parte confiable. 45 En el contexto del Cloud Computing, los potenciales clientes deberían comprobar si los proveedores de servicios Cloud pueden suministrar una copia de este certificado de la tercera parte o incluso una copia del informe de auditoría verificando la certificación, incluyendo lo referente a los requisitos indicados en esta Opinión". Ver también A.29WP05/2012, Sección 4.2, Pág.22.

49 A.29WP05/2012, Sección 3.4.2 Pág.13. Por favor, tener en cuenta que el PSC está obligado de facto a ayudar al cliente en la facilitación del ejercicio de los derechos de los datos de los interesados y a garantizar que sucede lo mismo con sus subcontristas.

Describir los procesos existentes para gestionar y responder a las peticiones de revelación de datos de carácter personal por parte de las autoridades competentes, con especial atención al procedimiento de notificación a los clientes a menos que existan prohibiciones al respecto como las existentes en la ley criminal para preservar la confidencialidad de la investigación de una autoridad competente.[50]

14. Compensaciones

Indicar las compensaciones que se efectuarán al cliente Cloud en el caso de que el PSC y/o sus subcontratistas incumplan sus obligaciones contractuales derivadas PLA, así como las compensaciones contractuales existentes en el caso de fallos en el cumplimiento de las estipulaciones sobre seguridad, monitorización, notificación de violaciones de la seguridad, portabilidad de datos y/o obligaciones de retención de datos. Las compensaciones podrían incluir ciertos tipos de daños, créditos de servicio y/o penalizaciones contractuales (financieros o de otro tipo, incluyendo la capacidad de demandar al PSC).[51]

15. Reclamaciones

Suministrar los datos de contacto del representante del PSC que recibirá las preguntas o reclamaciones con respecto a las prácticas de tratamiento de datos de carácter personal.

Suministrar los datos de contacto de la tercera parte, si la hubiere, que puede ser contactada para ayudar a resolver un conflicto con el PSC, como una autoridad de protección de datos o un servicio de mediación o arbitraje.

16. Pólizas de seguros del PSC

Describir el alcance de las pólizas de Ciberseguros del PSC, incluyendo los seguros relativos a los fallos de seguridad.

50 A.29WP05/2012, Sección 3.4.2 Pág.13-14. Ver también la Guía ICO, Pág. 19-20.
51 A.29WP05/2012, Sección 3.4.2 Pág.12.

V. Anexo 1 al Esquema de Privacy Level Agreement

1. IDENTIDAD DEL PSC (Y DE SU REPRESENTANTE EN LA UE, SI ES EL CASO), SU FUNCIÓN, Y LA INFORMACIÓN DE CONTACTO DEL DELEGADO DE PROTECCIÓN DE DATOS/ DATA PRIVACY OFFICER (DPO) Y DEL DELEGADO DE SEGURIDAD DE LA INFORMACIÓN/ INFORMATION SECURITY OFICCER (ISO)	*Especificar:* • *Denominación del PSC, dirección y lugar de establecimiento;* • *Representante(s) local(es) (p.ej.: representante local en la UE);* • *Cuál es la función asumida en materia de protección de datos con respecto a los tratamientos relevantes (p.ej.: responsable, co- responsable conjunto, encargado o sub-encargado)* • *Datos de contacto del Delegado de Protección de Datos o Data Protection Officer (DPO), si no existiera un DPO, los datos de contacto de la persona a cargo de los asuntos de privacidad que atenderá las solicitudes del cliente.* • *Datos de contacto del responsable de la seguridad de la información o, si no hay un ISO, los datos de contacto de la persona competente en materia de seguridad que atenderá las solicitudes del cliente*
2. CATEGORÍAS DE DATOS PERSONALES QUE EL CLIENTE TIENE PROHIBIDO TRANSMITIR, O TRATAR EN LA NUBE	*Especifique, si es el caso, qué categorías de datos personales tiene el cliente prohibido transmitir o tratar en la nube (por ejemplo, los datos relacionados con la salud).*
3. FORMAS EN LAS QUE LOS DATOS SERÁN TRATADOS	*Si el PSC es un encargado del tratamiento, se debe incluir información detallada sobre el alcance y las modalidades en las que el cliente responsable del tratamiento poder dar instrucciones al PSC encargado del tratamiento.* *En su caso, diferenciar entre las actividades llevadas a cabo en nombre del cliente para proporcionar el (los) servicio (s) acordado (s) en la nube (por ejemplo, el almacenamiento de datos), las actividades llevadas a cabo a petición del cliente (por ejemplo, la preparación o producción de informes), y las llevadas a cabo por iniciativa del PSC (por ejemplo, copias de seguridad, recuperación ante desastres, monitorización del fraude).* *Especificar cómo se informará al cliente de servicios en la nube sobre los cambios pertinentes en relación con el (los) servicio (s) acordado (s), tales como la implementación de funciones adicionales* *3.a - Ubicación de los datos personales* *Especifique la (s) ubicación (es) de todos los centros de datos donde pueden ser tratados los datos personales, y, en particular, dónde y cómo se podrán almacenar, duplicar en espejo, respaldados, y recuperados.* *3.b - Subcontratistas*

	Identificar los subcontratistas y sub-encargados que participan en el tratamiento de datos, la cadena de responsabilidades, y el enfoque utilizado para garantizar que se cumplen los requerimientos de protección de datos. *Identificar los procedimientos utilizados para informar al cliente de los cambios previstos en relación con la inclusión o sustitución de los subcontratistas o sub-encargados, manteniendo en todo momento los clientes responsables del tratamiento la posibilidad de oponerse a estos cambios, o de dar por terminado el contrato.* *3.c - Instalación de software en el sistema del cliente de servicios en la nube* *Indicar si la prestación del servicio requiere de la instalación de software en el sistema del cliente (p. ej. plug-ins del navegador) y sus implicaciones desde una perspectiva de protección de datos y seguridad.*
4. TRANSFERENCIA DE DATOS	*Indicar si los datos pueden ser transferidos, copiados y /o recuperados de forma transfronteriza, en el curso normal de las operaciones o ante una emergencia. Si dicha transferencia está restringida por las leyes aplicables, identificar el fundamento jurídico en el que se sustenta dicha transferencia (incluyendo transferencias sucesivas a través de varios niveles de subcontratistas).* *Indique si los datos se han de trasladar fuera del Espacio Económico Europeo. Si dicha transferencia tiene lugar, identificar en qué fundamento jurídico se sustenta: p. ej. Decisión de adecuación, clausulas tipo, (Safe Harbor) o Binding Corporate Rule´s (BCR´s).*
5. MEDIDAS DE SEGURIDAD	*Especificar las medidas técnicas, físicas y organizativas implementadas para proteger los datos personales contra la destrucción, accidental o ilícita, y la pérdida accidental; alteración, uso, modificación, difusión o acceso no autorizados; y contra toda forma ilícita de tratamiento.* *Describir las medidas técnicas, físicas y organizativas concretas que aseguren:* • *Disponibilidad: describir los procesos y medidas implementadas para gestionar el riesgo de interrupción y prevenir, detectar y reaccionar ante incidentes, por ejemplo, copias de seguridad de los enlaces de Internet, almacenamiento redundante y mecanismos efectivos de creación y recuperación de copias de seguridad;* • *Integridad: describir cómo asegura el proveedor de servicios la integridad (por ejemplo, detectando alteraciones en los datos personales mediante mecanismos criptográficos, tales como códigos de autenticación de mensajes o firmas);* • *Confidencialidad: describir cómo asegura el proveedor de servicios la confidencialidad, desde un punto de vista técnico (por ejemplo, mediante el cifrado de los datos "en tránsito" y "en reposo",25 mecanismos de autorización y autenticación fuertes26) y desde un punto de vista contractual, mediante acuerdos o cláusulas de confidencialidad, y políticas empresariales vinculantes tanto para el proveedor de servicios o sus empleados (a tiempo completo o parcial, o contratados) como para sus subcontratistas (en su caso) que puedan acceder a los datos, para asegurar que sólo las personas autorizadas tienen acceso a los datos;*

	• *Transparencia: describir qué medidas técnicas, físicas y organizativas ha implementado el proveedor de servicios para apoyar la transparencia y permitir su revisión por los clientes (véanse, por ejemplo, los apartados 6 y 7);* • *Aislamiento (limitación de la finalidad): describir cómo presta aislamiento el proveedor (por ejemplo, la adecuada gobernanza de los derechos y roles de acceso los datos personales (revisados periódicamente), gestión de accesos basada en el principio del mínimo privilegio, mejora de los hipervisores y la correcta gestión de los recursos compartidos si se utilizan máquinas virtuales para compartir recursos físicos entre diferentes clientes);* • *Capacidad de intervención: describir cómo permite el proveedor a los interesados ejercitar sus derechos de acceso, rectificación, cancelación, bloqueo y oposición; de cara a demostrar la ausencia de obstáculos técnicos y organizativos en relación con dichas obligaciones, incluyendo aquellos casos en que los datos sean tratados posteriormente por subcontratistas;* • *Portabilidad: véase el apartado 9;* • *Responsabilidad: véase el apartado 11.* *Especificar qué marcos de control de seguridad se han implementado (por ejemplo, ISO/IEC 27002, CSA CMM, ENISA, Information Assurance Framework, etc.) y qué controles específicos se han aplicado.*
6. SUPERVISIÓN	*Indicar si el cliente tiene la opción de monitorizar y/o auditar, en aras a asegurarse de que se cumplen con carácter permanente las medidas apropiadas de seguridad descritas en el PLA. Si tal supervisión es posible, especifíquese como (por ejemplo, mediante informes, auditorías).* *Especificar los controles que serán facilitados al cliente, así como los registros y auditorías de las correspondientes operaciones de tratamiento llevadas a cabo por el proveedor de servicios o sus subcontratistas.*
7. AUDITORÍAS DE TERCEROS	*Especificar si se facilitan al cliente informes de auditoría realizados por terceros independientes, y en qué medida, así como su ámbito de aplicación, la frecuencia con la que dichos informes se actualizan y si se entrega al cliente el informe completo o un resumen del mismo.* *Especificar si el auditor de la tercera parte confiable puede ser elegido por el cliente o por ambas partes, y quién pagará el coste de la auditoría.*
8. NOTIFICACIÓN DE UNA VIOLACIÓN DE LOS DATOS PERSONALES	*Una violación de los datos de carácter personal implica un fallo de seguridad que conduce a la pérdida, destrucción, alteración, revelación no autorizada o acceso, de forma accidental o ilegal, de datos de carácter personal transmitidos, almacenados o procesados de cualquier forma en conexión con la provisión de un servicio por parte de un PSC.* *Especificar si y cómo se informará al cliente de las violaciones de datos de carácter personal y de seguridad que afecten a los datos procesados por el PSC*

	y/o sus subcontratas, y dentro de qué marco temporal.
9. PORTABILIDAD DE DATOS, MIGRACIÓN, Y AYUDA EN LA TRANSFERENCIA DE VUELTA	*Especificar los formatos, la preservación de relaciones lógicas y cualquier coste asociado con la portabilidad de datos, aplicaciones y servicios.* *Describir si, cómo y a qué coste el PSC ayudará a los clientes en una posible migración de los datos a otro proveedor o de vuelta a un entorno TI propio.*
10. RETENCION DE DATOS, RESTABLECIMIENTO Y BORRADO	*Describir las políticas de retención de datos del PSC y las condiciones para devolver los datos de carácter personal y su destrucción una vez el servicio ha finalizado.* *10.a - Política de retención de datos* *Indicar durante cuánto tiempo se retendrán o podrán ser retenidos los datos de carácter personal.* *10.b - Borrado de datos* *Indicar los métodos disponibles o empleados para borrar los datos, y si los datos pueden ser retenidos después de que el cliente haya borrado (o solicitado su borrado), o después de la finalización del contrato. Indicar en cada caso el periodo durante el cual el PSC retendrá los datos.* *10.c – Retención de datos para el cumplimiento de requisitos legales* *Describir cómo el PSC cumple con los requisitos legales relativos a la retención de datos que se aplican tanto al PSC como al cliente.* *Indicar si y cómo el cliente puede solicitar al PSC que cumpla con normativas y leyes sectoriales específicas.*
11. RESPONSABILIDAD	*Describir qué políticas y procedimientos ha desplegado el PSC para garantizar y demostrar el cumplimiento legal, tanto por su parte, como por la de sus subcontratistas y socios de negocios, incluyendo la adopción de políticas internas y mecanismos que garanticen dicho cumplimiento legal (por ej. manteniendo documentación de todas las operaciones de procesado bajo su responsabilidad, y proporcionando una monitorización fiable y mecanismos de log exhaustivos).* *Identificar los certificados de auditoría relevantes de terceras partes obtenidos por el PSC, su fecha y su alcance.*
12. COOPERACIÓN	*Especificar cómo cooperará el PSC con el cliente Cloud para garantizar el cumplimiento legal de las disposiciones de protección de datos aplicables: por ej. para permitir que el cliente garantice el ejercicio de los derechos de sus usuarios (acceso, rectificación, cancelación, bloqueo y oposición) [Ver también la Sección*

	5: Capacidad de intervención]. *Describir cómo el PSC hará disponible al cliente y a las autoridades supervisoras la información necesaria para demostrar el cumplimiento legal.*
13. ACCESO DE LAS AUTORIDADES COMPETENTES	*Describir los procesos existentes para gestionar y responder a las peticiones de revelación de datos de carácter personal por parte de las autoridades competentes, con especial atención al procedimiento de notificación a los clientes a menos que existan prohibiciones al respecto como las existentes en la ley criminal para preservar la confidencialidad de la investigación de una autoridad competente.*
14. COMPENSACIONES	*Indicar las compensaciones que se efectuarán al cliente Cloud en el caso de que el PSC y/o sus subcontratistas incumplan sus obligaciones contractuales derivadas PLA, así como las compensaciones contractuales existentes en el caso de fallos en el cumplimiento de las estipulaciones sobre seguridad, monitorización, notificación de violaciones de la seguridad, portabilidad de datos y/o obligaciones de retención de datos. Las compensaciones podrían incluir ciertos tipos de daños, créditos de servicio y/o penalizaciones contractuales (financieros o de otro tipo, incluyendo la capacidad de demandar al PSC).*
15. RECLAMACIONES	*Suministrar los datos de contacto del representante del PSC que recibirá las preguntas o reclamaciones con respecto a las prácticas de tratamiento de datos de carácter personal.* *Suministrar los datos de contacto de la tercera parte, si la hubiere, que puede ser contactada para ayudar a resolver un conflicto con el PSC, como una autoridad de protección de datos o un servicio de mediación o arbitraje.*
16. POLIZAS DE SEGURO DEL PSC	*Describir el alcance de las pólizas de Ciberseguros del PSC, incluyendo los seguros relativos a los fallos de seguridad.*

