Anexo sobre el tratamiento de datos (anteriormente Anexo de SaaS)

Este Anexo sobre el tratamiento de datos (el "Data Processing Addendum" o «**DPA**») se incorpora al acuerdo de software o al acuerdo de servicios (el «**Contrato**») entre el Proveedor y el Cliente para la adquisición de determinadas licencias de Software SaaS o de servicios de Mantenimiento o de servicios profesionales (para los fines de este DPA, en adelante los «**Servicios**»), y forma parte de un contrato escrito (incluido en formato electrónico) entre el Proveedor y el Cliente. Todos los términos con mayúscula inicial no definidos en el presente documento tendrán el significado establecido en el Contrato.

1. **Definiciones.** Los términos con mayúscula inicial no definidos en el contexto o en el Acuerdo tendrán los significados que se les asignan a continuación:
   a) «***Responsable del tratamiento***» se refiere a la persona física o jurídica, autoridad pública, agencia u otro organismo que, solo o junto con otros, determina los fines y los medios del Tratamiento de datos personales.
   b) «***Leyes de protección de datos***» hace referencia a todas las leyes y reglamentos aplicables al Tratamiento de datos personales del Cliente en virtud del Contrato, incluidos, según corresponda: (i) la Ley de Privacidad del Consumidor de California, en su versión enmendada por la Ley de Derechos de Privacidad de California, así como cualquier reglamento vinculante promulgado en virtud de la misma (la «**CCPA**», por sus siglas en inglés); (ii) el Reglamento general de protección de datos (Reglamento [UE] 2016/679) (el «**RGPD de la UE**» o «**RGPD**»); (iii) la Ley federal suiza sobre protección de datos («**FADP**», por sus siglas en inglés); (iv) el RGPD de la UE en su versión aplicada a la legislación de Inglaterra y Gales, en virtud de la sección 3 de la Ley de la Unión Europea (retirada) de 2018 (el «**RGPD del RU**»); y (v) la Ley de Protección de Datos del Reino Unido de 2018; en cada caso, según sus versiones periódicamente actualizadas, enmendadas o sustituidas.
   c) «**Interesado**» se refiere a la persona física identificada o identificable con la que se relacionan los Datos personales del Cliente.
   d) «***Datos personales***» hace referencia a la información sobre una persona física identificada o identificable o que, de otro modo, constituye «datos personales», «información personal», «información de identificación personal» o términos similares, según se definen en las Leyes de protección de datos.
   e) «***Violación de la seguridad de los datos personales***» se refiere a la destrucción accidental o ilegal, pérdida, alteración, divulgación o acceso no autorizados de terceros a los Datos personales del Cliente que el Proveedor esté tratando, según sea el caso, por el cual un Responsable del tratamiento está obligado por las Leyes de protección de datos a notificarlo a las autoridades competentes de protección de datos o a los Interesados.
   f) «***Tratamiento***» se refiere a todas las operaciones que se lleven a cabo sobre los Datos personales, ya sea mediante medios automáticos o no, tales como la recopilación, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación mediante transmisión, distribución o puesta a disposición de otro modo, alineación o combinación, restricción, supresión o destrucción.
   g) «***Encargado del tratamiento***» se refiere a una persona física o jurídica, autoridad pública, agencia u otro organismo que Trata los Datos personales en nombre del Responsable del tratamiento.
   h) «***Cláusulas contractuales tipo***» o «**CCT de la UE**» se refiere a las Cláusulas contractuales tipo aprobadas por la Comisión Europea en la decisión 2021/914.
   i) «***Subencargado del tratamiento***» se refiere a las Filiales del Proveedor y a terceros contratados por el Proveedor (o por sus Filiales) para la prestación de una o todas las partes de los Servicios, y que trata los Datos personales del Cliente de acuerdo con este DPA.

2. **Tratamiento de los datos personales del Cliente**
   El Proveedor puede realizar el Tratamiento de los Datos personales del Cliente en virtud del Contrato como Encargado del tratamiento que actúa por cuenta del Cliente, el cual es el Responsable del tratamiento (o, según corresponda, el Proveedor podría actuar como subencargado, por cuenta del Cliente cuando este ultimo es considerado como el Encargado del tratamiento). El Proveedor se compromete a realizar el Tratamiento de los Datos personales con el único fin de cumplir con las obligaciones del Proveedor con el Cliente en virtud y de conformidad con (i) este DPA y el Contrato, y (ii) las instrucciones por escrito del Cliente, o (iii) para cumplir con las obligaciones del Proveedor en virtud de las leyes aplicables, sujeto a cualquier requisito de notificación en virtud de las Leyes de Protección de Datos. Los detalles del objeto del Tratamiento, su duración, naturaleza y finalidad, así como el tipo de Datos personales del Cliente y los Interesados, son los especificados en el Contrato; en caso de no especificarse, serán los establecidos en el Anexo 1 del Apéndice del presente DPA. El Cliente y el Proveedor aceptan cumplir con sus respectivas obligaciones en virtud de las Leyes de protección de datos aplicables a los Datos personales que se tratan en relación con los Servicios. El Cliente tiene la responsabilidad exclusiva de cumplir con las Leyes de protección de datos relativas al Tratamiento de los Datos personales del Cliente antes de divulgar, transferir o poner a disposición de otro modo cualquier Dato personal al Proveedor. El Proveedor informará inmediatamente al Cliente si, en su opinión, las instrucciones del Cliente infringen las Leyes de protección de datos.

3. **Seguridad del tratamiento**
   a) **Políticas generales de seguridad**. El Proveedor deberá aplicar y mantener medidas, procedimientos y prácticas técnicas y organizativas que correspondan a la naturaleza de los Datos personales del Cliente, y que estén diseñados para proteger la seguridad, confidencialidad, integridad y disponibilidad de los Datos personales del Cliente, así como para protegerlos frente a las Violaciones de la seguridad de los Datos personales, de conformidad con las medidas de seguridad del Proveedor a las que se hace referencia en el Contrato y que se describen con más detalle en: https://www.oneidentity.com/legal/security.aspx (en conjunto, el «***Sitio de seguridad***»), incluidas las siguientes:
      - la Política de seguridad de la información;
      - la Declaración de medidas técnicas y organizativas;
      - la Política de respuesta a una violación de la seguridad de los datos; y
      - la Política de privacidad.

El Proveedor puede modificar su Sitio de seguridad siempre que no reduzca significativamente el nivel general de protección proporcionado.

b) **Confidencialidad.** El Proveedor deberá proteger los Datos personales del Cliente de acuerdo con sus obligaciones de confidencialidad según lo establecido en el Contrato. El Proveedor deberá asegurarse de que el personal del Proveedor que realiza el Tratamiento de los Datos personales del Cliente haya celebrado acuerdos de confidencialidad por escrito con el Proveedor. El Proveedor deberá asegurarse de que dichas obligaciones de confidencialidad subsistan tras la finalización de la relación laboral de dicho personal. El Proveedor deberá formar periódicamente a las personas que tengan acceso a los Datos personales del Cliente sobre los requisitos y los principios de seguridad y privacidad de los datos.

4. Solicitudes de los Interesados.

A petición del Cliente, el Proveedor utilizará medidas comercialmente razonables para ayudar al Cliente a cumplir con sus obligaciones en virtud de las Leyes de protección de datos a fin de responder a las solicitudes de personas físicas para ejercer sus derechos en virtud de dichas Leyes de protección de datos, siempre que el Cliente no pueda cumplir razonablemente con esas solicitudes de forma independiente (incluso mediante el uso de los Servicios). Si el Proveedor recibe una solicitud de un Interesado en relación con los Datos personales que se tratan en virtud del presente, el Proveedor aconsejará al Interesado (cuando el Interesado haya proporcionado información para identificar al Cliente) que redirija su solicitud al Cliente.

5. Derechos de auditoría.

a) **Registros de proveedores en general.** El Proveedor deberá mantener registros de su Tratamiento de conformidad con las Leyes de protección de datos y, previa solicitud por escrito del Cliente, pondrá a disposición de este todos los registros razonablemente necesarios para demostrar el cumplimiento de las obligaciones del Proveedor en virtud del presente DPA y de las Leyes de protección de datos aplicables.

b) **Programa de cumplimiento de terceros.** El Proveedor deberá describir sus programas de auditoría y certificación de terceros (si corresponde) y hará copias resumidas de sus informes de auditoría (cada uno de ellos, un «**Informe de auditoría**»), que pondrá a disposición del Cliente previa solicitud por escrito de este (sujeto a las obligaciones de confidencialidad establecidas en el Acuerdo). El Cliente puede compartir una copia de los Informes de auditoría con las autoridades gubernamentales pertinentes, según sea necesario.

c) **Auditoría del cliente.** El Cliente puede realizar, a su cargo, una auditoría de conformidad con un plan acordado mutuamente que sea coherente con los criterios de auditoría que se indican a continuación (una «**Auditoría**»). El Cliente podrá ejercer sus derechos de Auditoría: (1) en la medida en que la aportación por parte del Proveedor de un Informe de auditoría no proporcione información suficiente para que el Cliente verifique el cumplimiento por parte del Proveedor del presente DPA o el cumplimiento de las Leyes de protección de datos; o (2) según sea necesario para que el Cliente responda a una auditoría de una autoridad gubernamental; o (3) en relación con una Violación de la seguridad de los datos personales.

Cada Auditoría deberá: (1) llevarla a cabo un tercero independiente, que deberá haber firmado un acuerdo de confidencialidad con el Proveedor; (2) limitarse a los aspectos razonablemente necesarios para que el Cliente evalúe el cumplimiento del Proveedor con este DPA y el cumplimiento de las partes con las Leyes de protección de datos; (3) realizarse en una fecha y hora mutuamente acordadas, y solo durante el horario laboral normal del Proveedor; (4) tener lugar como máximo una vez al año (salvo que lo exijan de otro modo las Leyes de protección de datos o que sea en relación con una violación de la seguridad de los datos personales); (5) abarcar únicamente las instalaciones controladas por el Proveedor; (6) limitar las conclusiones a los Datos personales del Cliente; y (7) tratar los resultados como información confidencial en la medida máxima en que lo permitan las Leyes de protección de datos.

6. Subencargados y transferencias internacionales.

a) **Uso de subencargados.** El Cliente generalmente autoriza al Proveedor a contratar a Subencargados en relación con la prestación de los Servicios. El Proveedor formalizará los acuerdos escritos apropiados con los Subencargados de conformidad con las disposiciones de este DPA y con las instrucciones del presente entre el Cliente y el Proveedor. El Proveedor es responsable de cualquier incumplimiento de este DPA en la medida en que sea causado por Subencargados contratados por el Proveedor.

b) **Lista de subencargados.** El Proveedor mantiene listas de Subencargados por Producto de software, incluidas sus funciones y ubicaciones, que están disponibles para el Cliente a través del registro en https://support.oneidentity.com/subprocessor. Al menos treinta (30) días antes de autorizar a cualquier nuevo Subencargado del tratamiento a acceder a los Datos personales, el Proveedor actualizará la lista de Subencargados y lo notificará al Cliente por correo electrónico en el momento del registro.

c) **Objeción a nuevos subencargados.** Si el Cliente no aprueba a un nuevo Subencargado, podrá rescindir cualquier suscripción al Software SaaS correspondiente enviando, antes de que finalice el periodo de preaviso, una notificación de rescisión por escrito que incluya una explicación de los motivos por los que no da su aprobación.

d) **Transferencias internacionales.** Para la transferencia de Datos personales europeos o del Reino Unido a un Subencargado del tratamiento que se encuentre en un tercer país que no ofrezca la protección adecuada para los Datos personales, el Proveedor y el Subencargado correspondiente deberán haber suscrito las Cláusulas contractuales tipo a fin de proporcionar las garantías adecuadas para la transferencia de dichos Datos personales de conformidad con las Leyes de protección de datos europeas y del Reino Unido.

7. Notificación de violación de la seguridad de los datos personales.

Además de las obligaciones establecidas en el Sitio de seguridad, el Proveedor deberá notificar sin demora indebida en cuanto tenga conocimiento de cualquier Violación de la seguridad de los datos personales y proporcionará la información que razonablemente pueda estar en su poder para ayudar al Cliente a cumplir con las obligaciones de este último de notificar una Violación de la seguridad de los datos personales conforme exige la Ley de protección de datos. El Proveedor puede proporcionar dicha información por fases a medida que esté disponible. El Proveedor se compromete a esforzarse de buena

fe por identificar la causa de una Violación de la seguridad de los datos personales, y a tomar las medidas que considere necesarias y razonables para subsanar la causa de dicha Violación de la seguridad de los datos personales.

8. **Eliminación de los datos personales del cliente.**
Salvo que el Cliente lo notifique al Proveedor al menos treinta (30) días antes de la finalización de los Servicios, tras la rescisión o el vencimiento del Contrato el Proveedor eliminará de sus sistemas todos los Datos personales del Cliente. El Proveedor realizará la eliminación de acuerdo con las prácticas de eliminación segura estándar del sector. Sin perjuicio de lo anterior, el Proveedor podrá conservar los Datos personales del Cliente: (i) según lo exijan las Leyes de protección de datos; o (ii) de conformidad con sus políticas estándar de copia de seguridad o conservación de registros, siempre que, en cualquiera de los casos, el Proveedor (1) mantenga la confidencialidad de los Datos personales del Cliente guardados y cumpla las disposiciones aplicables del presente Contrato con respecto a los mismos, y (2) no vuelva a tratar los Datos personales del Cliente conservados, salvo para los fines y durante el plazo especificados en las Leyes de protección de datos aplicables.

9. **Evaluación del impacto de la protección de datos.**
El Proveedor proporcionará al Cliente la cooperación y la asistencia que bien pudieran parecer razonables en la medida en que sea necesario para cumplir con la obligación del Cliente en virtud de las Leyes de protección de datos para llevar a cabo una evaluación del impacto de la protección de datos o una evaluación de riesgos similar relacionada con el uso de los Servicios por parte del Cliente.

APÉNDICE AL DPA

Este Apéndice forma parte del DPA.

ANEXO I – Objeto y detalles de Tratamiento

A. RELACIÓN DE LAS PARTES

El Contrato entre el Cliente, como Responsable del tratamiento, y el Proveedor, como Encargado del tratamiento, incluye una descripción de toda la información necesaria, como:

- nombre, dirección, nombre de la persona de contacto;
- cargo y datos de contacto;
- actividades relacionadas con los datos transferidos en virtud de estas Cláusulas; y
- fecha y firma.

B. DESCRIPCIÓN DEL TRATAMIENTO

1. Categorías de Interesados cuyos datos personales se tratan

Salvo que el Cliente lo indique de otro modo, los Datos personales tratados se relacionan con las siguientes categorías de Interesados:

- empleados, contratistas, socios comerciales del Cliente.

2. Categorías de Datos personales tratados

El Cliente determina las categorías de datos según su uso de los Servicios. Los Datos personales tratados generalmente se refieren a las siguientes categorías de datos:

- datos de empleo (que pueden incluir el nombre y la dirección de la empresa, el puesto de trabajo, la categoría y los datos demográficos y de ubicación) relativos a empleados del Cliente u otros terceros cuya información personal sea facilitada por el Cliente o en su nombre;
- información del sistema relacionada con los sistemas del Cliente o con los sistemas que el Cliente proporciona al Proveedor, y que está relacionada con los Servicios adquiridos en virtud del Contrato y es necesaria para la prestación de los Servicios (que puede incluir el ID de usuario y la contraseña, el nombre del ordenador y del dominio, la dirección IP, el número GUID o la ubicación del ordenador u otro dispositivo utilizado).

Los Datos personales del Cliente tratados pueden referirse a socios/ partner comerciales pasados, presentes y potenciales, o bien a otras personas relacionadas con dichos socios comerciales.

3. Datos sensibles tratados (si procede)

El Cliente no deberá proporcionar categorías especiales de datos personales (datos sensibles) salvo que se identifiquen caso por caso y solo en la medida en que las partes acuerden que dichas categorías especiales de datos deben estar cubiertas por la prestación de los Servicios.

4. Frecuencia del Tratamiento (por ejemplo, si los datos se tratan de forma puntual o continua)

De forma continua durante el uso de los Servicios.

5. Naturaleza del Tratamiento

a) Para los Servicios de mantenimimento : el Proveedor o sus Subencargados prestan asistencia cuando un Cliente envía una solicitud de asistencia porque el Software no está disponible o no funciona como se esperaba. Asimismo, responden a las llamadas telefónicas y realizan tareas básicas de resolución de problemas, además de gestionar las solicitudes de asistencia en un sistema de seguimiento.
b) Para los servicios profesionales : el Proveedor o sus Subencargados prestan Servicios sujetos al Pedido de servicios profesionales.
c) Para los software SaaS: suministro del Software SaaS adquirido por el Cliente.

6. Fines de la transferencia de datos y su Tratamiento posterior

Los Datos personales del Cliente que vienen tratados por Proveedor estarán sujetos a las siguientes actividades básicas de tratamiento:

a) uso de los Datos Personales para prestar los Servicios del Proveedor y, en su caso, para proporcionar acceso al Software SaaS y ventajas del mismo de conformidad con el Contrato, y para prestar Servicios de mantenimimento a petición del Cliente y conforme a los requisitos específicos del Cliente, según proceda, todo ello de conformidad con las instrucciones que se describen a continuación;
b) almacenamiento de los Datos personales;
c) tratamiento informático de los Datos personales para su transmisión;
d) mejora continua de las características y funcionalidades del servicio proporcionadas como parte de los Servicios del Proveedor, incluidos la automatización, el tratamiento de las transacciones y el aprendizaje automático;
e) ejecución de las instrucciones del Cliente de conformidad con el Acuerdo.

Las siguientes actividades de tratamiento adicionales se aplican a los Datos personales almacenados en el Software SaaS:

a) almacenamiento de los Datos personales en centros de datos (arquitectura multiusuario);

b) copia de seguridad y restauración de los Datos personales del Cliente almacenados en el software SaaS;
c) tratamiento informático de los Datos personales, incluidos la transmisión de datos, la recuperación de datos y el acceso a los datos;
d) comunicaciones a los usuarios del Cliente;
e) lanzamiento, desarrollo y carga de cualquier corrección o actualización del Software SaaS;
f) acceso a la red para permitir la transferencia de los Datos personales;
g) supervisión, resolución de problemas y administración de la infraestructura y la base de datos subyacentes del Software SaaS;
h) supervisión de la seguridad, la detección de intrusiones en la red y pruebas de penetración; y
i) según sea necesario, respuesta y atención a las solicitudes y demandas de los Interesados, según proceda y de conformidad con las instrucciones descritas a continuación.

El Proveedor puede utilizar datos anonimizados (que no sean Datos personales del Cliente, pero que puedan derivarse de los mismos) para fines relacionados con la mejora de los productos y el desarrollo de nuevos Productos y Servicios del Proveedor.

En la Documentación del Producto y la Guía de seguridad correspondientes se indican más detalles sobre las funciones del Software SaaS, la forma en que dicho software trata los Datos personales y la ubicación del almacenamiento de los mismos.

7. Período durante el cual se conservarán los Datos personales o, en su defecto, los criterios utilizados para determinar dicho período

Los Datos personales se tratarán durante el uso de los Servicios por parte del Cliente de conformidad con el Contrato y sujeto a la Sección 8 de este DPA.

8. En relación con las transferencias a (Sub)encargados, se debe especificar también el objeto, la naturaleza y la duración del Tratamiento

Con respecto a lasCláusulas contractuales tipo, las transferencias a los Subencargados se realizarán sobre la misma base que se establece en este DPA.

9. Instrucciones y compromisos del Cliente y el Proveedor.

El Proveedor seguirá las instrucciones escritas y documentadas que reciba del Cliente con respecto a los Datos personales del Cliente salvo que, en opinión del Proveedor, dichas instrucciones: (1) estén legalmente prohibidas o puedan dar lugar a una infracción de la Ley de protección de datos aplicable; (2) requieran cambios sustanciales en los Servicios del Proveedor; o (3) sean incompatibles con los términos del Contrato o con la Documentación del Proveedor en relación con los Servicios vendidos en virtud del presente. En tal caso, el Proveedor informará inmediatamente al Cliente de su incapacidad para seguir dichas instrucciones. Cualquier descripción del Tratamiento en el Contrato, en este DPA y en cualquier Documentación relacionada del Proveedor, se considerará como instrucciones del Cliente.

ANEXO II – Declaración de medidas técnicas y organizativas

El Proveedor utilizará las medidas técnicas y organizativas apropiadas establecidas en el Sitio de seguridad (como se define en la Sección 3 (a) del DPA) para el Tratamiento de los Datos personales del Cliente por parte del Proveedor en virtud del presente DPA. El Cliente acepta que el Proveedor puede modificar las medidas tomadas para proteger los Datos personales del Cliente siempre que no disminuya sustancialmente el nivel general de protección de datos acordado en el presente documento.