ANEXO SOBRE EL PROCESAMIENTO DE DATOS DE COMMAND ALKON INCORPORATED

Actualizado: 31/07/25

Este Anexo sobre el tratamiento de datos («DPA») forma parte del *Contrato marco de licencia y servicios* («Contrato») entre: (i) el Cliente (identificado en el Contrato marco de licencia y servicios) y sus filiales («Cliente»); y (ii) Command Alkon Incorporated y sus filiales («Empresa»), solo cuando lo exija el Reglamento general de protección de datos («RGPD») u otra legislación aplicable en materia de privacidad.

Este DPA sustituye cualquier acuerdo anterior entre las partes en relación con el objeto del presente documento, es decir, la privacidad y la seguridad de los datos según lo aplicable a las Leyes de Protección de Datos (definidas a continuación).

En consideración de las obligaciones mutuas establecidas en el presente documento, las partes acuerdan que los términos y condiciones que se establecen a continuación se añadirán como anexo al Acuerdo.

1. Definiciones

«Datos **personales del** cliente» se refiere a los datos personales tratados por la Empresa en nombre del Cliente en el marco de la prestación de los productos y/o servicios.

«CCPA» significa la Ley de Privacidad del Consumidor de California, modificada por la Ley de Derechos de Privacidad de California o cualquier otra legislación o normativa de California.

«Interesado» se refiere a la persona física a la que se refieren los Datos personales del cliente.

«Marco **de privacidad de** datos» o «DPF» se refiere al marco jurídico de la UE y EE. UU. para las transferencias transfronterizas de datos personales entre la Unión Europea y los Estados Unidos, e incluye la extensión del Reino Unido al DPF de la UE y EE. UU. y el DPF de Suiza y EE. UU.

«Leyes **de protección de** datos» se refiere a todas las leyes y reglamentos aplicables relacionados con el tratamiento de datos personales y la privacidad que puedan existir en las jurisdicciones pertinentes, incluyendo, cuando proceda, el Reglamento General de Protección de Datos (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos, y por el que se deroga la Directiva 95/46/CE («RGPD») (y cualquier modificación o sustitución de la misma), la Ley Federal Suiza de Protección de Datos («FADP») (y cualquier modificación o sustitución de la misma), el RGPD de la UE, modificado e incorporado a la legislación del Reino Unido en virtud de la Ley del Reino Unido sobre la Unión Europea (Retirada) de 2018 y la legislación secundaria aplicable promulgada en virtud de dicha Ley («RGPD del Reino Unido») (y cualquier modificación o sustitución de la misma), la Ley de Protección de la Información Personal y de los Documentos Electrónicos de Canadá («PIPEDA») (y cualquier modificación o sustitución de la misma), la Ley General de Protección de Datos de Brasil (la «LGPD») (y cualquier modificación o sustitución de la misma), la Ley de Privacidad de 1988

(Cth) de Australia, en su versión modificada («Ley de Privacidad de Australia») (y cualquier modificación o sustitución de la misma), las leyes estatales de privacidad de los Estados Unidos (incluidas la CCPA y la CPRA de California) en su versión vigente o modificada, o cualquier otra legislación aplicable en materia de privacidad que exija un DPA. Cuando se mencione específicamente el RGPD, se aplicarán los mismos requisitos a cualquier otro requisito equivalente de la Ley de Protección de Datos aplicable.

«Datos personales» significa cualquier información relacionada con un interesado, incluyendo, entre otros, el nombre, el número de identificación, los datos de localización, el identificador en línea o uno o varios factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social del interesado.

«Tratamiento» o «Tratar» significa cualquier operación o conjunto de operaciones realizadas sobre los Datos personales del cliente, ya sea por medios automatizados o no, como la recogida, el registro, la organización, la estructuración, el almacenamiento, la alteración, la recuperación, la consulta, el uso, la divulgación, la eliminación, la restricción, el acceso, la difusión, la combinación, la adaptación, la copia, la transferencia, el borrado y/o la destrucción de los Datos personales del cliente.

«Violación **de la** seguridad» significa una violación confirmada de la seguridad que da lugar a la destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilícito a los Datos personales del Cliente transmitidos, almacenados o tratados de cualquier otra forma.

«Cláusulas contractuales tipo» o «SCC» se refiere a los requisitos contractuales estándar establecidos en la Ley de Protección de Datos aplicable (Cláusulas contractuales tipo de la UE, Cláusulas contractuales modelo iberoamericanas para la transferencia internacional de datos personales, Cláusulas contractuales modelo de la ASEAN para el flujo transfronterizo de datos, Cláusulas contractuales modelo de Hong Kong para la transferencia transfronteriza de datos personales, Cláusulas contractuales tipo de la SDAIA para la transferencia de datos personales, etc.).

«Tercero» significa una parte distinta del Cliente o la Empresa.

Los términos «responsable del tratamiento», «encargado del tratamiento» y «**autoridad de** control», tal y como se utilizan en el presente DPA, tendrán el significado que se les atribuye en la Ley de Protección de Datos aplicable.

Todos los demás términos no definidos pero escritos con mayúscula inicial tendrán el significado establecido en el Acuerdo o en la Ley de Protección de Datos aplicable.

2. Tratamiento de los datos personales del cliente

2.1 Finalidad del tratamiento. La finalidad del tratamiento de datos en virtud del presente DPA es la prestación de los productos y/o servicios de conformidad con el Acuerdo. El anexo 1 describe el objeto y los detalles del tratamiento de los datos personales del cliente.

2.2 Responsabilidades del encargado del tratamiento y del responsable del tratamiento. Las partes reconocen y acuerdan que: (a) La Empresa es un encargado del tratamiento

de los Datos personales del Cliente en virtud de las Leyes de protección de datos; (b) El Cliente es un responsable del tratamiento de los Datos personales del Cliente en virtud de las Leyes de protección de datos; (c) el Cliente es responsable de obtener todas las autorizaciones y aprobaciones necesarias para introducir, utilizar, proporcionar, almacenar y tratar los Datos personales del cliente a fin de que la Empresa pueda proporcionar los productos y/o servicios; y (d) cada parte cumplirá con las obligaciones que le sean aplicables en virtud de las Leyes de protección de datos con respecto al Tratamiento de los Datos personales del cliente.

2.3 Leyes de Protección de Datos de EE. UU. A los efectos de las Leyes de Protección de Datos de EE. UU. (incluida la CCPA), «responsable del tratamiento» incluye «empresa»; «encargado del tratamiento» incluye «proveedor de servicios»; «interesado» incluye «consumidor»; y «Datos Personales» incluye «información personal». La Empresa es un proveedor de servicios y el Cliente es una empresa.

2.4 Instrucciones del Cliente. El Cliente instruye a la Empresa para que trate los Datos Personales del Cliente: (a) de conformidad con el Acuerdo y cualquier Suplemento aplicable; (b) según sea necesario para proporcionar los productos y/o servicios al Cliente; (c) según sea necesario para cumplir con la legislación o normativa aplicable; y (d) para cumplir con otras instrucciones razonables por escrito proporcionadas por el Cliente, siempre que dichas instrucciones sean coherentes con los términos del Acuerdo. El Cliente se asegurará de que sus instrucciones para el Tratamiento de los Datos Personales del Cliente cumplan con las Leyes de Protección de Datos. Entre las partes, el Cliente será el único responsable de la exactitud, calidad y legalidad de los Datos Personales del Cliente y de los medios por los que el Cliente obtuvo los Datos Personales del Cliente.

2.5 Cumplimiento de las instrucciones del Cliente por parte de la Empresa. La Empresa solo tratará los Datos Personales del Cliente de acuerdo con las instrucciones del Cliente y tratará los Datos Personales del Cliente como información confidencial. Si la Empresa cree o tiene conocimiento de que alguna de las instrucciones del Cliente entra en conflicto con cualquier Ley de Protección de Datos, la Empresa informará al Cliente en un plazo razonable. La Empresa podrá Tratar los Datos Personales del Cliente sin instrucciones escritas del Cliente si así lo exige la legislación aplicable a la que está sujeta la Empresa. En tal caso, la Empresa informará al Cliente de dicho requisito antes de Tratar los Datos Personales del Cliente, salvo que lo prohíba la legislación aplicable.

2.6 Tratamiento conforme a la CCPA. En la medida en que el Tratamiento de los Datos Personales por parte de la Empresa esté sujeto a la CCPA, la Empresa certifica que no: (a) conservar, utilizar o divulgar los Datos personales del Cliente salvo en los casos previstos en el Acuerdo, cuando sea necesario para proporcionar los productos y/o servicios, para crear o mejorar la calidad de los productos y/o servicios, para detectar incidentes de seguridad, para proteger contra actividades fraudulentas o ilegales, para conservar subencargados del tratamiento de conformidad con el presente ATD, o en la medida en que lo permita la CCPA; ni (b) vender o compartir los Datos personales del Cliente.

3. Subencargados del tratamiento

3.1 Nombramiento de subencargados del tratamiento. Por la presente, el Cliente otorga autorización general por escrito a la Empresa para que contrate a terceros subencargados del tratamiento para prestar servicios limitados o auxiliares en relación con el suministro de productos y/o servicios. El sitio web de la Empresa enumera los subencargados del tratamiento que actualmente contrata la Empresa para llevar a cabo actividades de tratamiento específicas relacionadas con los Datos personales del cliente (https://commandalkon.com/sub-processor-list/) y la Empresa actualizará la lista de subencargados del tratamiento antes de contratar a cualquier nuevo subencargado del tratamiento para llevar a cabo un tratamiento específico. El Cliente puede suscribirse para recibir actualizaciones electrónicas cada vez que se modifique la lista de subencargados del tratamiento de la Empresa, enviando una solicitud a través de la página de subencargados del tratamiento de la Empresa (enlace anterior) o enviando dicha solicitud aprivacy@commandalkon.com . El Cliente puede oponerse a cualquier subencargado del tratamiento comunicando dicha oposición a la Empresa en un plazo de treinta (30) días a partir de la actualización, y las partes trabajarán de buena fe para resolver la oposición. El Cliente acepta por la presente las actividades de subprocesamiento realizadas por los subprocesadores actuales que figuran en el sitio web de la Empresa.

3.2 Seguridad del subencargado del tratamiento. Cuando la Empresa subcontrate sus obligaciones, lo hará únicamente mediante un acuerdo escrito con el subencargado del tratamiento que imponga obligaciones contractuales al menos equivalentes a las impuestas a la Empresa en virtud del presente ATD. Las partes acuerdan que las copias de los acuerdos con los subencargados del tratamiento autorizados que deban facilitarse de conformidad con las cláusulas contractuales tipo aplicables se facilitarán únicamente previa solicitud por escrito del Cliente.

3.3 Responsabilidad. Cuando el subencargado del tratamiento incumpla sus obligaciones de protección de datos en virtud de dicho acuerdo escrito, la Empresa seguirá siendo plenamente responsable ante el Cliente del cumplimiento de las obligaciones del subencargado del tratamiento en virtud de dicho acuerdo.

4. Responsabilidades de seguridad de la Empresa

4.1 Seguridad de la empresa. La empresa implementará las medidas técnicas y organizativas adecuadas para salvaguardar los datos personales del cliente («Programa **de seguridad de la** información»), teniendo en cuenta el estado de la técnica, los costes de implementación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como el riesgo de probabilidad y gravedad variables para los derechos y libertades de las personas físicas. La empresa se rige por las siguientes normas de seguridad: SOC 2; NIST 800-171; AWS CIS.

4.2 Seguridad del Cliente. El Cliente reconoce que los productos y/o servicios incluyen ciertas características y funcionalidades que el Cliente puede optar por utilizar y que afectan a la seguridad de los Datos Personales del Cliente tratados por el Cliente mediante el uso de los productos y/o servicios. El Cliente es responsable de revisar la información que la Empresa pone a su disposición en relación con la seguridad de los datos y de determinar de forma independiente si los productos y/o servicios cumplen

los requisitos y las obligaciones legales del Cliente, incluidas sus obligaciones en virtud de la Ley de Protección de Datos aplicable. El Cliente es además responsable de configurar adecuadamente los productos y/o servicios y de utilizar las características y funcionalidades puestas a su disposición por la Empresa para mantener la seguridad adecuada en función de la naturaleza de los Datos personales del Cliente tratados como resultado del uso de los productos y/o servicios por parte del Cliente. El Cliente es responsable del uso que haga de los productos y/o servicios y del almacenamiento de cualquier copia de los Datos Personales del Cliente fuera de los sistemas de la Empresa o de los subencargados del tratamiento de la Empresa, incluyendo, entre otros, la protección de las credenciales de autenticación de la cuenta, los sistemas y dispositivos, y la conservación de copias de los Datos Personales del Cliente según corresponda.

4.3 Personal de la empresa. La empresa se asegurará de que su personal involucrado en el procesamiento de los datos personales de los clientes esté informado de la naturaleza confidencial de dichos datos, haya recibido la formación adecuada sobre sus responsabilidades y esté sujeto a obligaciones de confidencialidad, las cuales seguirán vigentes tras la finalización de la relación de dicha persona con la empresa.

4.4 Pruebas de seguridad. La empresa comprobará, evaluará y valorará la eficacia del programa de seguridad de la información para garantizar el tratamiento seguro de los datos personales del cliente. La empresa cumplirá su programa de seguridad de la información y declara y garantiza que dicho programa cumple y seguirá cumpliendo la legislación aplicable.

4.5 Evaluaciones de impacto. La Empresa tomará medidas razonables para cooperar y ayudar al Cliente a realizar evaluaciones de impacto y consultas relacionadas con cualquier autoridad supervisora si el Cliente está obligado a realizar dichas evaluaciones de impacto en virtud de las Leyes de Protección de Datos.

5. Derechos de los interesados

5.1 Asistencia con las obligaciones del Cliente. En la medida en que el Cliente, en su uso o recepción de los productos y/o servicios, no tenga la capacidad de corregir, modificar, restringir, bloquear o eliminar los Datos Personales del Cliente según lo exijan las Leyes de Protección de Datos, la Empresa cumplirá sin demora con las solicitudes razonables del Cliente para facilitar dichas acciones en la medida en que la Empresa esté legalmente autorizada y sea capaz de hacerlo. Si lo permite la ley, el Cliente será responsable de cualquier coste derivado de la prestación de dicha asistencia por parte de la Empresa.

5.2 Obligaciones de notificación. La Empresa, en la medida en que lo permita la ley, notificará sin demora al Cliente si recibe una solicitud de un Interesado para acceder, corregir, modificar, eliminar u oponerse al Tratamiento de los Datos Personales del Cliente relacionados con dicho individuo. La Empresa no responderá a ninguna solicitud de este tipo relacionada con los Datos Personales del Cliente sin el consentimiento previo por escrito del Cliente, salvo para confirmar que la solicitud se refiere al Cliente. Además, la Empresa, en la medida en que lo permita la ley, notificará sin demora al Cliente si recibe una solicitud de divulgación o correspondencia, notificación u otra comunicación relacionada con los Datos

Personales del Cliente por parte de las fuerzas del orden, una autoridad competente o una autoridad de protección de datos pertinente. La Empresa prestará al Cliente la cooperación y asistencia razonables y adecuadas en relación con la tramitación de cualquier solicitud de este tipo, en la medida en que lo permita la ley y en la medida en que el Cliente no tenga acceso a dichos Datos personales del cliente a través del uso o la recepción de los productos y/o servicios. Si lo permite la ley, el Cliente será responsable de cualquier coste derivado de la prestación de dicha asistencia por parte de la Empresa.

6. Violación de datos personales

6.1 Obligaciones de notificación. En caso de que la Empresa tenga conocimiento de una Violación de la Seguridad verificada que afecte a los Datos Personales del Cliente, la Empresa notificará al Cliente dicha Violación de la Seguridad sin demora indebida y, en cualquier caso, en un plazo máximo de setenta y dos (72) horas tras su confirmación. Las obligaciones del presente apartado 6 no se aplicarán a los incidentes causados por el Cliente, el personal del Cliente o los usuarios finales, ni a los intentos fallidos o actividades que no comprometan la seguridad de los Datos personales del Cliente, incluidos los intentos fallidos de inicio de sesión, pings, escaneos de puertos, ataques de denegación de servicio y otros ataques de red a cortafuegos o sistemas en red.

6.2 Forma de notificación. La notificación de las violaciones de seguridad, si las hubiera, se enviará al punto de contacto del Cliente por correo electrónico o por teléfono. Es responsabilidad exclusiva del Cliente asegurarse de que mantiene información de contacto precisa en los sistemas de asistencia de la Empresa en todo momento. El Cliente es el único responsable de cumplir con los requisitos de notificación de violaciones aplicables al Cliente y de cumplir con cualquier obligación de notificación a terceros relacionada con cualquier violación de la seguridad de los datos personales.

6.3 Contenido de la notificación. Cuando sea necesaria una notificación, esta deberá incluir, como mínimo y en la medida de lo posible:

6.3.1 describir la naturaleza de la Violación de la Seguridad, las categorías y el número de Interesados afectados, y las categorías y el número de registros de Datos Personales afectados;

6.3.2 comunicar el nombre y los datos de contacto de la persona de contacto pertinente de la Empresa a la que se puede obtener más información;

6.3.3 describir las posibles consecuencias de la Violación de la Seguridad; y

6.3.4 describir las medidas adoptadas o propuestas para hacer frente a la violación de la seguridad.

7. Supresión o devolución de los datos personales de los clientes

7.1 Eliminación o devolución. Con sujeción a la sección 7.3, la Empresa se compromete a eliminar de forma segura los Datos personales del cliente, o bien, previa solicitud por escrito del Cliente, a devolver una copia completa de todos y cada uno de los Datos

personales del cliente mediante transferencia segura de archivos en el formato que el Cliente considere razonable, en un plazo máximo de treinta (30) días a partir de la fecha de cese de cualquier servicio que implique el Tratamiento de Datos personales del cliente (la «Fecha de cese»).

7.2 Certificación por escrito. Si el Cliente y la Empresa han celebrado Cláusulas Contractuales Tipo que exigen la certificación de la eliminación por escrito (como las cláusulas 8.5 y 16 de las CCT de la UE), las partes acuerdan que la certificación por escrito solo se proporcionará previa solicitud por escrito del Cliente.

7.3 Definición de «Eliminar». A efectos aclaratorios, «Eliminar» significa suprimir o borrar los Datos personales del Cliente de tal forma que no puedan recuperarse ni reconstruirse.

7.4 Registros. La Empresa podrá conservar los Datos personales del cliente en la medida en que lo exijan las leyes aplicables o lo establezca el calendario de conservación de documentos de la Empresa, siempre que la Empresa garantice la confidencialidad de todos esos Datos personales del cliente.

8. Derechos de auditoría de la « »

8.1 Derechos de auditoría. El Cliente podrá contratar, con una frecuencia máxima de una vez al año, a un tercero de mutuo acuerdo para auditar los Datos personales del Cliente con el único fin de cumplir sus requisitos de auditoría de conformidad con el artículo 28, apartado 3, letra h), del RGPD o cualquier disposición equivalente de la Ley de Protección de Datos aplicable. Para solicitar una auditoría, el Cliente deberá presentar un plan de auditoría detallado con al menos cuatro (4) semanas de antelación a la fecha propuesta para la auditoría, en el que se describa el alcance, la duración y la fecha de inicio de la misma. Las solicitudes de auditoría deben enviarse aprivacy@commandalkon.com . El auditor deberá firmar un acuerdo de confidencialidad por escrito aceptable para la Empresa antes de realizar la auditoría. La auditoría deberá realizarse durante el horario laboral habitual, con sujeción a las políticas de la Empresa, y no podrá interferir de manera injustificada en las actividades comerciales de la Empresa. Cualquier auditoría correrá a cargo exclusivo del Cliente. La Empresa cooperará con cualquier solicitud de auditoría del Cliente o de cualquier autoridad reguladora o supervisora competente para verificar el cumplimiento por parte de la Empresa de sus obligaciones en virtud del presente DPA, poniendo a disposición, con sujeción a las obligaciones de confidencialidad, los informes de auditoría de terceros, cuando estén disponibles, y/o las descripciones de los controles de seguridad y cualquier otra información que el Cliente solicite razonablemente en relación con las prácticas y políticas de seguridad de la Empresa.

8.2 Asistencia en materia de cumplimiento. Teniendo en cuenta la naturaleza del Tratamiento y la información de que dispone la Empresa, esta prestará la cooperación y asistencia adecuadas y razonables al Cliente en relación con las obligaciones de cumplimiento del Cliente descritas en los artículos 32 a 36 del RGPD.

9. Transferencias de datos

9.1 Autorización general. El Cliente acepta que la Empresa pueda, con sujeción a la sección 9.2, almacenar y tratar los Datos personales del Cliente en los Estados Unidos de América y en cualquier otro país en el que la Empresa o cualquiera de sus subencargados del tratamiento mantenga instalaciones o trate Datos personales. Dichas transferencias se regirán en primer lugar por la certificación del Marco de Privacidad de Datos de la Empresa o, alternativamente, por las Cláusulas Contractuales Tipo entre filiales de la Empresa. La Empresa no transferirá, ni provocará la transferencia, de ningún dato personal del cliente de una jurisdicción a otra, salvo que lo haga de conformidad con la legislación aplicable, y no provocará que el cliente incumpla ninguna ley de protección de datos.

9.2 Cláusulas contractuales estándar de la UE. En la medida en que, y solo en la medida en que, la Empresa procese Datos personales del cliente procedentes del Espacio Económico Europeo y se requieran Cláusulas contractuales estándar, se aplicará el Módulo Dos de las Cláusulas contractuales estándar, que se incorporan por la presente. A los efectos de las Cláusulas contractuales estándar, el Cliente es el «exportador de datos» y la Empresa es el «importador de datos».

9.3 Anexo del Reino Unido a las cláusulas contractuales tipo de la UE. En la medida en que, y solo en la medida en que, la empresa procese datos personales de clientes del Reino Unido y se requieran cláusulas contractuales tipo, las partes acuerdan que el anexo del Reino Unido se aplicará a los datos personales que se transfieran a través de los productos y/o servicios desde el Reino Unido, ya sea directamente o mediante una transferencia posterior, a cualquier país o destinatario fuera del Reino Unido que no esté reconocido por la autoridad reguladora competente del Reino Unido o el organismo gubernamental del Reino Unido como un país que ofrece un nivel adecuado de protección de los datos personales.

9.4 FADP suizo. En la medida en que, y solo en la medida en que, la Empresa procese datos personales de clientes de Suiza, se aplicarán los siguientes requisitos adicionales en la medida en que las transferencias de datos estén sujetas exclusivamente a la FADP o estén sujetas tanto a la FADP como al RGPD de la UE: (a) el término «Estado miembro» no debe interpretarse de manera que excluya a los interesados en Suiza de la posibilidad de ejercer sus derechos en su lugar de residencia habitual (Suiza) de conformidad con la cláusula 18(c) de las Cláusulas Contractuales Tipo; (b) en la medida en que las transferencias de datos en las que se basan las cláusulas contractuales tipo estén sujetas exclusivamente a la LPD, las referencias al RGPD de la UE se entenderán como referencias a la LPD; y (c) en la medida en que las transferencias de datos en las que se basan las Cláusulas Contractuales Tipo estén sujetas tanto a la FADP como al RGPD de la UE, las referencias al RGPD de la UE se entenderán como referencias a la FADP en la medida en que las transferencias de datos estén sujetas a la FADP.

9.5 Otras cláusulas contractuales tipo o cláusulas contractuales modelo. En la medida en que, y solo en la medida en que, se produzca una transferencia de Datos personales del cliente distinta de las mencionadas anteriormente que requiera cláusulas contractuales tipo o cláusulas contractuales modelo específicas para cada país en

virtud de las Leyes de protección de datos aplicables, las partes acuerdan que las cláusulas contractuales tipo o cláusulas contractuales modelo específicas para cada país que sean necesarias se incorporarán automáticamente por referencia y formarán parte integrante del presente DPA.

9.6 Medidas complementarias. Como complemento a las Cláusulas Contractuales Estándar, si la Empresa tiene conocimiento de que cualquier autoridad gubernamental (incluidas las fuerzas del orden) desea obtener acceso o una copia de algunos o todos los Datos Personales del Cliente tratados por la Empresa, ya sea de forma voluntaria u obligatoria, para fines relacionados con la inteligencia de seguridad nacional, a menos que lo prohíba la ley o exista una obligación legal que exija lo contrario, la Empresa: 1) notificará inmediatamente al Cliente al que se refieren los Datos Personales; 2) informará a la autoridad gubernamental pertinente de que no ha sido autorizada a revelar los Datos personales del cliente y, a menos que lo prohíba la ley, deberá notificarlo inmediatamente al Cliente al que se refieren los Datos personales del cliente; 3) informará a la autoridad gubernamental de que debe dirigir todas las solicitudes o demandas directamente al Cliente al que se refieren los Datos personales del cliente; y 4) no proporcionará acceso a los Datos personales del cliente hasta que lo autorice por escrito el Cliente al que se refieren los Datos personales del cliente o hasta que se vea obligada a hacerlo por ley. Si se ve obligada a hacerlo por ley, la Empresa hará todo lo que sea razonable y legal para impugnar dicha prohibición u obligación. Si la Empresa se ve obligada a presentar los Datos personales del cliente, solo los revelará en la medida en que lo exija la ley, de conformidad con el proceso legal aplicable.

9.7 Ley de Vigilancia de Inteligencia Extranjera. La empresa no ha recibido anteriormente ninguna directiva en virtud del artículo 702 de la Ley de Vigilancia de Inteligencia Extranjera de los Estados Unidos, codificada en 50 U.S.C. §1881a («FISA, artículo 702»). Ningún tribunal ha determinado que la Empresa sea el tipo de entidad elegible para recibir procesos emitidos en virtud de la Sección 702 de la FISA. La Empresa no es el tipo de proveedor que puede ser objeto de recopilación ascendente («recopilación masiva») de conformidad con la Sección 702 de la FISA, tal y como se describe en la decisión *Schrems II*.

9.8 Precedencia de la transferencia. En caso de que los servicios estén cubiertos por más de un mecanismo de transferencia, la transferencia de los Datos personales del Cliente estará sujeta a un único mecanismo de transferencia de acuerdo con el siguiente orden de precedencia: (i) la certificación del Marco de privacidad de datos de la Empresa; (ii) las Cláusulas contractuales tipo aplicables (cuando lo exija la Ley de protección de datos aplicable).

10. Vigencia y rescisión

Vigencia del DPA. El presente DPA entrará en vigor en la fecha en que se ejecute íntegramente el Acuerdo y, sin perjuicio de la expiración de la vigencia de cualquier suscripción adquirida, seguirá en vigor hasta la eliminación de todos los Datos personales del Cliente, tal y como se describe en el presente DPA, y expirará automáticamente en ese momento.

11. Incumplimiento; Recursos; Partes

11.1 Limitación de la responsabilidad. La responsabilidad de la Empresa por el incumplimiento de sus obligaciones en el presente DPA está sujeta a la disposición de limitación de responsabilidad del Acuerdo.

11.2 Partes del presente DPA. Nada de lo dispuesto en el DPA conferirá ningún beneficio o derecho a ninguna persona o entidad que no sea parte del presente DPA.

12. Condiciones generales

Legislación aplicable y jurisdicción

12.1 El presente DPA se revisará según sea necesario en función de las circunstancias.

12.2 Sin perjuicio de lo dispuesto en las cláusulas 7 (Mediación y jurisdicción) y 9 (Legislación aplicable) de las Cláusulas Contractuales Tipo:

12.2.1 las partes del presente AED se someten a la jurisdicción estipulada en el Acuerdo con respecto a cualquier controversia o reclamación que surja en relación con el presente AED , incluidas las controversias relativas a su existencia, validez o rescisión; y

12.2.2 el presente AED y todas las obligaciones extracontractuales o de otro tipo que se deriven de él o estén relacionadas con él se regirán por las leyes del país o territorio estipulado a tal efecto en el Acuerdo.

Orden de prelación

12.3 En caso de conflicto o inconsistencia entre este DPA y las Cláusulas Contractuales Tipo cuando estas sean necesarias, prevalecerán las Cláusulas Contractuales Tipo.

12.4 Sin perjuicio de lo dispuesto en los apartados 12.2 y 12.3, en lo que respecta al objeto del presente DPA, en caso de incoherencias entre las disposiciones del presente DPA y cualquier otro acuerdo entre las partes, incluido el Acuerdo y incluidos (salvo que se acuerde expresamente lo contrario por escrito, firmado en nombre de las partes) los acuerdos celebrados o que se pretenda celebrar después de la fecha del presente DPA, prevalecerán las disposiciones del presente DPA.

Cambios en las leyes de protección de datos

12.5 El Cliente podrá:

12.5.1 mediante notificación por escrito a la Empresa con al menos treinta (30) días naturales de antelación, proponer cualquier modificación de las Cláusulas Contractuales Tipo que sea necesaria como consecuencia de cualquier cambio en la Ley de Protección de Datos o de cualquier decisión de una autoridad competente en virtud de dicha ley; y

12.5.2 proponer cualquier otra modificación del presente DPA que el Cliente considere razonablemente necesaria para cumplir los requisitos de cualquier Ley de Protección de Datos.

12.6 Si el Cliente notifica lo dispuesto en la sección 12.5, las partes discutirán sin demora las modificaciones propuestas y negociarán de buena fe con el fin de acordar y aplicar dichas modificaciones o modificaciones alternativas destinadas a cumplir los requisitos identificados en la notificación del Cliente tan pronto como sea razonablemente posible.

Divisibilidad

12.7 Si alguna disposición del presente DPA fuera inválida o inaplicable, el resto del DPA seguirá siendo válido y vigente. La disposición inválida o inaplicable: (i) se modificará según sea necesario para garantizar su validez y aplicabilidad, preservando en la medida de lo posible las intenciones de las partes o, si esto no fuera posible; (ii) se interpretará de manera que la parte inválida o inaplicable nunca haya estado incluida en el presente documento.

Anexo I: Detalles del tratamiento de datos

Exportador de datos (responsable del tratamiento): El cliente identificado en el Acuerdo.

Importador de datos (encargado del tratamiento): La empresa identificada en el Acuerdo.

Objeto: El objeto del tratamiento de datos en virtud del presente DPA son los datos personales del cliente.

Duración del tratamiento: La duración del Acuerdo más el periodo hasta que la Empresa elimine todos los Datos personales del Cliente de conformidad con el presente DPA.

Finalidad: La finalidad del tratamiento de datos es la prestación de los productos y/o servicios al cliente.

Naturaleza del tratamiento: La naturaleza del tratamiento de datos es la prestación de los productos y/o servicios descritos en el Contrato y en el presente DPA.

Categorías de interesados: Empleados del Cliente y empleados de las filiales, clientes y socios comerciales del Cliente.

Tipos de datos personales: El Cliente puede cargar, enviar o proporcionar de cualquier otra forma determinados datos personales del Cliente a los productos y/o servicios, cuyo alcance suele determinar y controlar el Cliente a su entera discreción y que pueden incluir información de contacto; información sobre la interacción con el sitio web, los productos y los servicios; direcciones; fecha de nacimiento; lugar de nacimiento; direcciones de correo electrónico; nombres; sexo; cargo; números de teléfono; número de permiso de conducir; firma; número de empleado; información de geolocalización; salario; nombre de usuario; contraseña; información sobre el rendimiento; cualificaciones y restricciones; información sobre el dispositivo.

Datos sensibles transferidos: Ninguno.

Frecuencia de la transferencia: De forma continua, según sea necesario para la prestación de los productos y/o servicios.

Transferencias a subencargados del tratamiento: Según se describe en el presente DPA y en la lista de subencargados del tratamiento de la empresa, disponible en . Registros de las actividades de tratamiento disponibles previa solicitud.

Autoridad de control competente: Según lo determinado por las leyes de protección de datos aplicables o, por orden de efectividad, 1) de conformidad con los términos del Acuerdo o 2) la Autoridad de Protección de Datos de los Países Bajos.

Conservación: De conformidad con el Acuerdo y el presente DPA.

Medidas técnicas y organizativas: Las medidas de seguridad técnicas y organizativas implementadas por el Importador de Datos se describen en la sección 4.1 del DPA. Se puede solicitar información adicional.