

# ANEXO DE PROCESAMIENTO DE DATOS DE COMMAND ALKON INCORPORATED

Actualizado: 25/07/24

Este Anexo de procesamiento de datos (" **DPA** ") forma parte del Acuerdo *Maestro de Licencia y Servicios* (" **Acuerdo** ") entre: (i) el Cliente (identificado en el Acuerdo Maestro de Licencia y Servicios) y sus filiales del EEE (" **Cliente** "); y (ii) Command Alkon Incorporated y sus filiales (" **Compañía** ") solo cuando lo requiera el Reglamento General de Protección de Datos (" **GDPR** ") u otra privacidad aplicable legislación.

Este Anexo reemplaza cualquier acuerdo previo entre las partes con respecto al tema del presente documento, es decir, la privacidad y seguridad de los datos según sea aplicable a la legislación de privacidad.

En consideración de las obligaciones mutuas establecidas en el presente documento, las partes acuerdan que los términos y condiciones establecidos a continuación se agregarán como un Anexo al Acuerdo.

## 1. Definiciones

"**Datos personales del cliente**" se refiere a los datos personales procesados por la Compañía en nombre del Cliente en la provisión 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 por otra legislación/regulación de California.

"**Sujeto de los datos**" significa la persona con la que se relacionan los Datos personales del cliente.

"**Marco de privacidad de datos**" significa el marco legal UE-EE. UU. para las transferencias transfronterizas de datos personales entre la Unión Europea y los Estados Unidos e incluye la Extensión del Reino Unido a la EU-EE. UU. DPF y Suiza-Estados Unidos DPF.

"**Leyes de protección de datos**" significa todas las leyes y regulaciones aplicables relacionadas con el procesamiento de datos personales y privacidad que puedan existir en las jurisdicciones pertinentes, incluyendo, cuando corresponda, el Reglamento General de Protección de Datos (UE) 2016/679 sobre la protección de personas físicas con respecto al procesamiento de datos personales y sobre la libre circulación de dichos datos, y derogando la Directiva 95/46/CE ("GDPR") (y cualquier enmienda o reemplazo a la misma), la Ley Federal Suiza sobre Protección de datos ("FADP") (y cualquier enmienda o reemplazo al mismo), el RGPD de la UE enmendado e incorporado a la ley del Reino Unido bajo la Ley de Retirada de la Unión Europea del Reino Unido de 2018 y la legislación secundaria aplicable hecha bajo esa Ley ("GDPR del Reino Unido") (y cualquier enmienda o reemplazo a la misma), la Ley de Protección de Datos Personales y Documentos Electrónicos de Canadá ("PIPEDA") (y cualquier enmienda o reemplazo a la misma), la Ley General de Protección de Datos de Brasil (la "LGPD") (y cualquier enmienda o reemplazo a la misma), la Ley de Privacidad de 1988 (Cth) de Australia, en su forma enmendada ("Ley de Privacidad

Australiana”) (y cualquier enmienda o reemplazo a la misma), la Ley de Privacidad de EE. las leyes estatales de privacidad (incluidas la CCPA y la CPRA de California) tal como se hayan emitido o enmendado, o cualquier otra legislación de privacidad aplicable que requiera un DPA. Donde se menciona 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 sujeto de datos, incluyendo pero no limitado a un nombre, un número de identificación, datos de ubicación, un identificador en línea o uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social del sujeto de datos.

“**Proceso**” o “**Procesamiento**” significa cualquier operación o conjunto de operaciones que se realice en los Datos Personales del Cliente, ya sea por medios automatizados o no, como la recopilación, grabación, organización, estructuración, almacenamiento, alteración, recuperación, consulta, uso, divulgación, eliminación, restricción, acceso, difusión, combinación, adaptación, copia, transferencia, eliminación y/o destrucción de los Datos Personales del Cliente.

“**Infracción de seguridad**” significa una violación confirmada de seguridad que conduce a una destrucción accidental o ilegal, pérdida, alteración, divulgación no autorizada o acceso a los Datos personales del cliente transmitidos, almacenados o procesados de otra manera.

“**Cláusulas Contractuales Estándar**” significa los requisitos contractuales estándar establecidos en virtud de la Ley de Protección de Datos aplicable (Cláusulas Contractuales Estándar de la UE, Cláusulas Contractuales Modelo de la Junta Latinoamericana de Protección de Datos de RIPD, Cláusulas Contractuales Modelo de la ASEAN, etc.).

“**Tercero**” significa una parte que no sea el Cliente o la Compañía.

Los términos “**controlador**”, “**procesador**” y “**autoridad supervisora**” tal como se usan en este DPA tendrán los significados que se les atribuyen en la Ley de Protección de Datos aplicable.

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

## **2. Procesamiento de Datos Personales del Cliente**

2.1 Propósito del procesamiento. El propósito del procesamiento de datos bajo este DPA es la provisión de los productos y/o servicios de conformidad con el Acuerdo. El Anexo 1 describe el tema y los detalles del Procesamiento de Datos Personales del Cliente.

2.2 Responsabilidades del procesador y del controlador. Las partes reconocen y acuerdan que: (a) la Compañía es un procesador de Datos Personales del Cliente bajo las Leyes de Protección de Datos; (b) El Cliente es un controlador de Datos Personales del Cliente bajo las Leyes de Protección de Datos; (c) El Cliente es responsable de obtener todas las autorizaciones y aprobaciones necesarias para ingresar, usar, proporcionar, almacenar y procesar los Datos Personales del Cliente para permitir que la Compañía proporcione los productos y/o servicios; y (d) cada parte cumplirá con

las obligaciones aplicable a él bajo las leyes de protección de datos con respecto al procesamiento de Datos personales del cliente.

- 2.3 Leyes de protección de datos de los Estados Unidos. A los efectos de las leyes de protección de datos de los Estados Unidos (incluida la CCPA), “controlador” incluye “negocios”; “procesador” incluye “proveedor de servicios”; “sujeto de datos” incluye “consumidor”; y “Datos personales” incluye “información personal”. La compañía es un proveedor de servicios y el cliente es un negocio.
- 2.4 Instrucciones para el cliente. El Cliente indica a la Compañía que procese los Datos Personales del Cliente: (a) de acuerdo 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 ley o regulación aplicable; y (d) para cumplir con otras instrucciones razonables por escrito proporcionadas por el Cliente cuando dichas instrucciones sean consistentes con los términos del Acuerdo. El cliente se asegurará de que sus instrucciones para el procesamiento 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 los medios por los cuales el Cliente obtuvo los Datos Personales del Cliente.
- 2.5 Cumplimiento de las instrucciones del cliente por parte de la compañía. La Compañía solo procesará los Datos Personales del Cliente de acuerdo con las instrucciones del Cliente y tratará los Datos Personales del Cliente como información confidencial. Si la Compañía cree o se da cuenta de que alguna de las instrucciones del Cliente entra en conflicto con alguna Ley de Protección de Datos, la Compañía deberá informar al Cliente dentro de un plazo razonable. La Compañía puede Procesar Datos Personales del Cliente que no sean las instrucciones escritas del Cliente si así lo requiere la ley aplicable a la que la Compañía está sujeta. En esta situación, la Compañía informará al Cliente de dicho requisito antes de que la Compañía procese los Datos Personales del Cliente, a menos que lo prohíba la ley aplicable.
- 2.6 Procesamiento CCPA. En la medida en que el procesamiento de datos personales de la Compañía esté sujeto a la CCPA, la Compañía certifica que no deberá: (a) conservar, usar o divulgar Datos personales del cliente que no sean los previstos en el Acuerdo, según sea necesario para proporcionar los productos y/o servicios, construir o mejorar la calidad de los productos y/o servicios, detectar incidentes de seguridad, proteger contra actividades fraudulentas o ilegales, retener subprocesadores de acuerdo con este DPA, o de otra manera permitido por la CCPA; o (b) vender o compartir Datos personales del cliente.

### **3. Subprocesadores**

- 3.1 Nombramiento de subprocesadores. Por el presente, el cliente proporciona una autorización general por escrito para que la Compañía contrate subprocesadores externos para proporcionar servicios limitados o auxiliares en relación con la provisión de productos y/o servicios. El sitio web de la Compañía enumera los subprocesadores contratados actualmente por la Compañía para llevar a cabo actividades de procesamiento específicas relacionadas con los Datos personales del cliente (<https://commandalkon.com/sub-processor-list/>) y la Compañía actualizará la

lista de subprocesadores antes de contratar a cualquier nuevo subprocesador para llevar a cabo un procesamiento específico. El cliente puede registrarse para recibir actualizaciones electrónicas cada vez que cambie la lista de subprocesadores de la Compañía enviando dicha solicitud a [privacy@commandalkon.com](mailto:privacy@commandalkon.com). El cliente puede oponerse a cualquier subprocesador comunicando dicha objeción a la Compañía dentro de los treinta (30) días posteriores a la actualización, y las partes trabajarán de buena fe para resolver la objeción. Por el presente, el cliente acepta subprocesar las actividades de los subprocesadores actuales que figuran en el sitio web de la Compañía.

- 3.2 Seguridad del subprocesador. Cuando la Compañía subcontrate sus obligaciones, lo hará solo por medio de un acuerdo escrito con el subprocesador que impone obligaciones contractuales que son al menos equivalentes a las obligaciones impuestas a la Compañía bajo este Anexo. Las partes acuerdan que las copias de los acuerdos con subprocesadores autorizados que deben proporcionarse de conformidad con las Cláusulas Contractuales Estándar aplicables se proporcionarán solo a solicitud por escrito del Cliente.
- 3.3 Responsabilidad. Cuando el subprocesador no cumpla con sus obligaciones de protección de datos en virtud de dicho acuerdo escrito, la Compañía seguirá siendo totalmente responsable ante el Cliente por el cumplimiento de las obligaciones del subprocesador en virtud de dicho acuerdo.

#### **4. Responsabilidades de seguridad**

- 4.1 Seguridad de la compañía. La compañía implementará las medidas técnicas y organizativas apropiadas para salvaguardar los Datos Personales del Cliente (“**Programa de Seguridad de la Información**”) teniendo en cuenta el estado de la técnica, los costos de implementación y la naturaleza, el alcance, el contexto y los propósitos del Procesamiento, así como el riesgo de variar la probabilidad y gravedad de los derechos y libertades de las personas físicas. La compañía se gobierna bajo los siguientes estándares de seguridad: 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 elegir usar que afectan la seguridad de los Datos personales del Cliente procesados por el uso del Cliente de los productos y/o servicios. El Cliente es responsable de revisar la información que la Compañía pone a disposición sobre su seguridad de datos y de tomar una determinación independiente sobre si los productos y/o servicios cumplen con los requisitos y obligaciones legales del Cliente, incluidas sus obligaciones bajo la Ley de Protección de Datos aplicable. El Cliente es además responsable de configurar correctamente los productos y/o servicios y de utilizar las características y funcionalidades puestas a disposición por la Compañía para mantener la seguridad adecuada a la luz de la naturaleza de los Datos Personales del Cliente procesados como resultado del uso de los productos y/o servicios por parte del Cliente. El Cliente es responsable de su uso de los productos y/o servicios y de su almacenamiento de cualquier copia de los Datos Personales del Cliente fuera de los sistemas de la Compañía o de los subprocesadores de la Compañía, incluyendo, pero no limitado a,

asegurar las credenciales de autenticación de la cuenta, sistemas y dispositivos, y retener copias de sus Datos personales del cliente según corresponda.

- 4.3 Personal de la compañía. La Compañía se asegurará de que su personal involucrado en el Procesamiento de Datos Personales del Cliente sea informado de la naturaleza confidencial de los Datos Personales del Cliente, haya recibido la capacitación adecuada sobre sus responsabilidades y esté sujeto a obligaciones de confidencialidad, y tales obligaciones sobrevivirán a la terminación del compromiso de esa persona con la Compañía.
- 4.4 Pruebas de seguridad. La compañía probará, evaluará y evaluará la efectividad del Programa de Seguridad de la Información para garantizar el Procesamiento seguro de los Datos Personales del Cliente. La compañía cumplirá con su Programa de Seguridad de la Información y representa y garantiza que su Programa de Seguridad de la Información cumple y cumplirá con la ley aplicable.
- 4.5 Evaluaciones de impacto. La compañía 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 bajo las Leyes de Protección de Datos.

## **5. Derechos del sujeto de datos**

- 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, enmendar, restringir, bloquear o eliminar los Datos Personales del Cliente según lo requieran las Leyes de Protección de Datos, la Compañía deberá cumplir de inmediato con las solicitudes razonables del Cliente para facilitar tales acciones en la medida en que la Compañía esté legalmente permitida y pueda hacerlo. Si se permite legalmente, el Cliente será responsable de cualquier costo que surja de la provisión de dicha asistencia por parte de la Compañía.
- 5.2 Obligaciones de notificación. La Compañía, en la medida en que lo permita legalmente, notificará de inmediato al Cliente si recibe una solicitud de un Interesado para acceder, corregir, enmendar, eliminar u objetar el Procesamiento de los Datos Personales del Cliente relacionados con dicha persona. La Compañía no responderá a ninguna solicitud del Sujeto de Datos relacionados con los Datos Personales del Cliente sin el consentimiento previo por escrito del Cliente, excepto para confirmar que la solicitud se relaciona con el Cliente. Además, la Compañía, en la medida en que lo permita legalmente, notificará de inmediato al Cliente si recibe una solicitud de divulgación o correspondencia, notificación u otra comunicación relacionada con los Datos Personales del Cliente de parte de la policía, una autoridad competente o una autoridad de protección de datos relevante. La Compañía proporcionará al Cliente la cooperación y asistencia adecuadas y razonables en relación con el manejo de dicha solicitud, en la medida en que lo permita legalmente y en la medida en que el Cliente no tenga acceso a dichos Datos Personales del Cliente a través de su uso o recepción de los productos y/o servicios. Si se permite legalmente, el Cliente será responsable de cualquier costo que surja de la provisión de dicha asistencia por parte de la Compañía.

## 6. **Infracción de datos personales**

- 6.1 Obligaciones de notificación. En caso de que la Compañía tenga conocimiento de una Violación de Seguridad verificada que involucra Datos personales del cliente, la Compañía notificará al Cliente de la Infracción de Seguridad sin demoras indebidas y, en cualquier caso, a más tardar setenta y dos (72) horas después de la confirmación. Las obligaciones de esta Sección 6 no se aplican a incidentes causados por el personal del Cliente o del Cliente o los usuarios finales o a intentos o actividades fallidos que no comprometan la seguridad de los Datos Personales del Cliente, incluidos intentos fallidos de inicio de sesión, pings, escaneos de puertos, ataques de denegación de servicio y otros ataques de red en firewalls o sistemas en red.
- 6.2 Forma de notificación. La notificación de violaciones de seguridad, si las hubiera, se entregará al punto de contacto del Cliente por correo electrónico o por teléfono. Es responsabilidad exclusiva del Cliente asegurarse de que mantiene la información de contacto precisa sobre los sistemas de soporte de la Compañía en todo momento. El Cliente es el único responsable de cumplir con los requisitos de notificación de incumplimiento aplicables al Cliente y de cumplir con las obligaciones de notificación de terceros relacionadas con cualquier Violación de Seguridad de Datos Personales.
- 6.3 Contenido de la notificación. Cuando se requiera una notificación, dicha notificación deberá, como mínimo:
- 6.3.1 describir la naturaleza de la violación de seguridad, las categorías y el número de sujetos de datos en cuestión, y las categorías y números de registros de datos personales en cuestión;
  - 6.3.2 comunicar el nombre y los datos de contacto del contacto relevante de la Compañía de quien se puede obtener más información;
  - 6.3.3 describir las posibles consecuencias de la violación de seguridad; y
  - 6.3.4 describa las medidas tomadas o propuestas para hacer frente a la Infracción de Seguridad.

## 7. **Eliminación o devolución de datos personales del cliente**

- 7.1 Eliminar o devolver. Sujeto a la sección 7.3, la Compañía acepta de inmediato y en cualquier caso dentro de los treinta (30) días siguientes a la fecha de cese de cualquier servicio que implique el Procesamiento de Datos Personales del Cliente (la "**Fecha de Cese**"), Eliminar de forma segura los Datos Personales del Cliente o, a solicitud oportuna por escrito del Cliente, devolver una copia completa de todos y cada uno de los Datos Personales del Cliente al Cliente mediante transferencia segura de archivos en el formato que razonablemente lo solicite el Cliente.
- 7.2 Si el Cliente y la Compañía han firmado Cláusulas Contractuales Estándar que requieren la certificación de eliminación por escrito (como las Cláusulas 8 .5 y 16 de las SCC 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. Para aclaraciones, “**Eliminar**” significa eliminar u borrar los Datos Personales del Cliente de manera que no puedan ser recuperados o reconstruidos.
- 7.4 Registros. La Compañía puede conservar los Datos Personales del Cliente en la medida requerida por las Leyes Aplicables o según lo exija el programa de retención de documentos de la Compañía, siempre que la Compañía garantice la confidencialidad de todos esos Datos Personales del Cliente.

## **8. Derechos de auditoría**

- 8.1 Derechos de auditoría. No más de una vez al año, el Cliente puede contratar a un tercero mutuamente acordado para auditar a la Compañía únicamente con el propósito de cumplir con sus requisitos de auditoría de conformidad con el Artículo 28, Sección 3 (h) del RGPD. Para solicitar una auditoría, el Cliente debe presentar un plan de auditoría detallado al menos cuatro (4) semanas antes de la fecha de auditoría propuesta, describiendo el alcance propuesto, la duración y la fecha de inicio de la auditoría. Las solicitudes de auditoría deben enviarse a [privacy@commandalkon.com](mailto:privacy@commandalkon.com). El auditor debe ejecutar un acuerdo de confidencialidad por escrito aceptable para la Compañía antes de realizar la auditoría. La auditoría debe realizarse durante el horario comercial regular, sujeto a las políticas de la Compañía, y no puede interferir irrazonablemente con las actividades comerciales de la Compañía. Cualquier auditoría es a los costos y gastos únicos del Cliente. La Compañía cooperará con cualquier Cliente o cualquier solicitud de auditoría de autoridad reguladora o supervisora competente para verificar el cumplimiento de la Compañía con sus obligaciones bajo este DPA poniendo a disposición, sujeto a obligaciones de no divulgación, informes de auditoría de terceros, cuando estén disponibles, y/o descripciones de controles de seguridad y otra información razonablemente solicitada por el Cliente con respecto a las prácticas y políticas de seguridad de la Compañía.
- 8.2 Asistencia para el cumplimiento. Teniendo en cuenta la naturaleza del Procesamiento y la información disponible para la Compañía, la Compañía brindará una cooperación y asistencia adecuadas y razonables al Cliente con respecto a las obligaciones de cumplimiento del Cliente descritas en los Artículos 32-36 del RGPD.

## **9. Transferencias de datos**

- 9.1 Autorización general. El cliente acepta que la Compañía puede, sujeto a la Sección 9.2, almacenar y procesar los Datos personales del cliente en los Estados Unidos de América y cualquier otro país en el que la Compañía o cualquiera de sus subprocesadores mantenga instalaciones o procese datos personales de otra manera. Cualquier transferencia de este tipo se registrará primero por la certificación del Marco de Privacidad de Datos de la Compañía o, alternativamente, por las Cláusulas Contractuales Estándar interafiliadas de la Compañía. La Compañía no transferirá, ni hará que se transfieran, ningún dato personal del cliente de una jurisdicción a otra a menos que de acuerdo con la ley aplicable y no causará que el Cliente infrinja ninguna Ley de Protección de Datos.
- 9.2 Cláusulas Contractuales Estándar. En la medida en que, y solo en la medida en que la Compañía procese los Datos Personales del Cliente del Espacio Económico Europeo

y se requieran Cláusulas Contractuales Estándar, se aplicará el Módulo Dos de las Cláusulas Contractuales Estándar y se incorporarán por la presente. Para los propósitos de las Cláusulas Contractuales Estándar, el Cliente es el “exportador de datos” y la Compañía es el “importador de datos”.

- 9.3 Anexo del Reino Unido a las Cláusulas Contractuales Estándar de la UE. En la medida en que, y solo en la medida en que la Compañía procese datos personales de clientes del Reino Unido y se requieran cláusulas contractuales estándar, 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 del Reino Unido, ya sea directamente o mediante transferencia posterior, a cualquier país o destinatario fuera del Reino Unido que no sea reconocido por la autoridad reguladora competente del Reino Unido o el organismo gubernamental para el Reino Unido como proveedor de un nivel adecuado de protección para Datos Personales.
- 9.4 FADP suizo. En la medida y solo en la medida en que la Compañía procese datos personales de clientes de Suiza, se aplicarán los siguientes requisitos adicionales en la medida en que las transferencias de datos estén exclusivamente sujetas al FADP o estén sujetas tanto al FADP como al RGPD de la UE: (a) el término “estado miembro” no debe interpretarse de tal manera que excluya a los sujetos de datos en Suiza de la posibilidad de demandar por 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 subyacentes a las Cláusulas Contractuales Estándar están sujetas exclusivamente al FADP, las referencias al RGPD de la UE deben entenderse como referencias al FADP; y (c) en la medida en que las transferencias de datos subyacentes a las Cláusulas Contractuales Estándar están sujetas tanto al FADP como al RGPD de la UE, las referencias al RGPD de la UE deben entenderse como referencias al FADP en la medida en que las transferencias de datos estén sujetas al FADP P.
- 9.5 Medidas Suplementarias. Como complemento a las Cláusulas Contractuales Estándar, si la Compañía se entera de que alguna autoridad gubernamental (incluida la policía) desea obtener acceso o una copia de algunos o todos los Datos Personales del Cliente procesados por la Compañía, ya sea de forma voluntaria o obligatoria, para fines relacionados con la inteligencia de seguridad nacional, entonces a menos que esté legalmente prohibido o bajo una obligación legal obligatoria que requiera lo contrario, la Compañía: 1) notificará inmediatamente al Cliente al que se aplican los Datos Personales; 2) informará la autoridad gubernamental pertinente que no ha sido autorizado a divulgar los Datos personales del cliente y, a menos que esté legalmente prohibido, deberá notificar inmediatamente al Cliente a quien se aplican los Datos personales del cliente; 3) informar a la autoridad gubernamental que debe dirigir todas las solicitudes o demandas directamente al Cliente al que se aplican los Datos personales del cliente; y 4) no proporcionar acceso a los Datos personales del cliente hasta que lo autorice por escrito el Cliente al que se aplican los Datos personales del cliente o hasta que lo obligue legalmente a hacerlo. Si se ve obligada legalmente a hacerlo, la Compañía hará esfuerzos razonables y legales para desafiar dicha prohibición o coacción. Si la Compañía se ve obligada a producir los Datos Personales del Cliente, la Compañía solo revelará los Datos Personales del Cliente en



la medida legalmente requerida para hacerlo de acuerdo con el proceso legal aplicable.

- 9.6 Ley de Vigilancia de Inteligencia Extranjera. La compañía no ha recibido previamente ninguna directiva bajo la Sección 702 de la Ley de Vigilancia de Inteligencia Extranjera de los Estados Unidos, codificada en 50 U.S.C. §1881a (“Sección FISA 702”). Ningún tribunal ha determinado que la Compañía sea el tipo de entidad elegible para recibir un proceso emitido bajo la Sección 702 de FISA. La compañía no es el tipo de proveedor que es elegible para ser objeto de recolección ascendente (recolección “a granel”) de conformidad con la Sección 702 de FISA como se describe en la decisión *Schrems II*.
- 9.7 Precedencia de transferencia. En el 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 Compañía; (ii) Cláusulas Contractuales Estándar aplicables (cuando así lo requiera la Ley de Protección de Datos aplicable).

## 10. Término y Terminación

Término de DPA. Este DPA entrará en vigor en la fecha en que se ejecute completamente el Acuerdo y, a pesar de la expiración del término de cualquier suscripción comprada, permanecerá vigente hasta la eliminación de todos los Datos Personales del Cliente, y caducará automáticamente después de la eliminación de todos los Datos Personales del Cliente tal como se describe en este DPA.

## 11. Incumplimiento; Remedios; Partes

- 11.1 Limitación de responsabilidad. La responsabilidad de la compañía por el incumplimiento de sus obligaciones en este DPA está sujeta a la disposición de limitación de responsabilidad en el Acuerdo.
- 11.2 Partes en este DPA. Nada en el DPA conferirá beneficios o derechos a ninguna persona o entidad que no sean las partes de este DPA.

## 12. Términos generales

*Ley aplicable y jurisdicción*

- 12.1 Este DPA se revisará un año a partir de la fecha de emisión y luego tres años después, o antes si es apropiado.
- 12.2 A menos que lo exijan las Cláusulas Contractuales Estándar:
- 12.2.1 las partes de este Anexo se someten a la elección de jurisdicción estipulada en el Acuerdo con respecto a cualquier disputa o reclamo que surja bajo este Anexo, incluidas las disputas relacionadas con su existencia, validez o terminación; y

12.2.2 este Anexo y todas las obligaciones no contractuales o de otro tipo que surjan de o estén relacionadas con él se rigen por las leyes del país o territorio estipuladas para este propósito en el Acuerdo.

*Orden de precedencia*

12.3 En caso de conflicto o inconsistencia entre este Anexo y las Cláusulas Contractuales Tipo en las que se requieran las Cláusulas Contractuales Estándar, prevalecerán las Cláusulas Contractuales Estándar.

12.4 Sujeto a la sección 12.2, con respecto al tema de este Anexo, en caso de inconsistencias entre las disposiciones de este Anexo y cualquier otro acuerdo entre las partes, incluido el Acuerdo e incluyendo (salvo que se acuerde explícitamente lo contrario por escrito, firmados en nombre de las partes) los acuerdos celebrados o pretendidos celebrarse después de la fecha de este Anexo, prevalecerán las disposiciones de este Anexo.

*Cambios en las leyes de protección de datos*

12.5 El cliente puede:

12.5.1 por al menos treinta (30) días naturales de notificación por escrito a la Compañía de vez en cuando, proponga cualquier variación a las Cláusulas Contractuales Estándar que se requiera como resultado de cualquier cambio o decisión de una autoridad competente en virtud de esa Ley de Protección de Datos; y

12.5.2 proponga cualquier otra variación a este Anexo que el Cliente considere razonablemente necesarias para abordar los requisitos de cualquier Ley de Protección de Datos.

12.6 Si el Cliente da aviso bajo la sección 12.5, las partes discutirán rápidamente las variaciones propuestas y negociarán de buena fe con el fin de acordar e implementar esas o variaciones alternativas diseñadas para abordar los requisitos identificados en el aviso del Cliente tan pronto como sea razonablemente posible.

*Incisión*

12.7 Si alguna disposición de este Anexo es inválida o inaplicable, entonces el resto de este Anexo seguirá siendo válido y vigente. La disposición inválida o inaplicable será: (i) enmendada según sea necesario para asegurar su validez y aplicabilidad, preservando al mismo tiempo las intenciones de las partes lo más cerca posible o, si esto no es posible; (ii) interpretada de una manera como si la parte inválida o inaplicable nunca hubiera sido contenida en ella.

## **Anexo I - Detalles del procesamiento de datos**

**Exportador de datos (Controlador):** Cliente identificado en el Acuerdo.

**Importador de datos (procesador):** Compañía tal como se identifica en el Acuerdo.

**Asunto:** El tema del procesamiento de datos bajo este DPA son los Datos personales del cliente.

**Duración del procesamiento:** El término del Acuerdo más el período hasta que la Compañía elimine todos los Datos Personales del Cliente de acuerdo con este DPA.

**Propósito:** El propósito del procesamiento de datos es la provisión de los productos y/o servicios al Cliente.

**Naturaleza del procesamiento:** La naturaleza del procesamiento de datos es para la provisión de los productos y/o servicios tal como se describe en el Acuerdo.

**Categorías de sujetos de datos:** empleados de clientes y empleados de afiliados de clientes, clientes y socios comerciales.

**Tipos de datos personales:** el cliente puede cargar, enviar o proporcionar de otra manera ciertos Datos personales del cliente a los productos y/o servicios, cuyo alcance generalmente es determinado y controlado por el Cliente a su exclusivo criterio y puede incluir información de contacto; sitio web, producto e información de interacción de servicios; direcciones; fecha de nacimiento; ubicación de nacimiento; direcciones de correo electrónico; nombres; género; título; números de teléfono; número de licencia de conducir; firma; número de empleado; información de ubicación geográfica; tasa de pago; nombre de usuario; contraseña; rendimiento información; calificaciones y restricciones; información del dispositivo.

**Datos confidenciales transferidos:** Ninguno.

**Frecuencia de la transferencia:** continua según sea necesario para la provisión de los productos y/o servicios.

**Transferencias a subprocesadores:** como se describe en la lista de subprocesadores de la Compañía, disponible en <https://commandalkon.com/sub-processor-list/>.

**Autoridad Supervisora Competente:** Según lo determinado por las Leyes de Protección de Datos aplicables o, por orden de efecto, 1) de acuerdo con los términos del Acuerdo o 2) Autoridad de Protección de Datos de los Países Bajos.

**Retención:** De acuerdo con el Acuerdo y este 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. Los detalles adicionales están disponibles a pedido.