APÉNDICE DE PROCESAMIENTO DE DATOS DE COMMAND ALKON INCORPORATED

Actualizado: 23/08/2023

Este Apéndice de Procesamiento de Datos («**DPA**») forma parte del *Principal Acuerdo de Licencia y Servicios («***Acuerdo**») celebrado entre: (i) el cliente (identificado en el Acuerdo Principal de Licencia y Servicios) y sus filiales del EEE (**«Cliente»**); y (ii) Command Alkon Incorporated y sus filiales («**Empresa**») solo cuando lo exija el Reglamento General de Protección de Datos («**GDPR**») o cualquier otra legislación aplicable en materia de confidencialidad.

Este Apéndice sustituye a cualquier acuerdo anterior entre las partes en relación con el tema abordado, a saber, la confidencialidad y la seguridad de los datos, de conformidad con la legislación de privacidad.

A la luz de las obligaciones mutuas establecidas en este documento, las partes acuerdan añadir los términos y condiciones que se indican a continuación como Anexo al Contrato.

1. Definiciones

Los «**Datos Personales del Cliente**» se refieren a los datos personales Procesados por la Empresa en nombre del Cliente en el contexto de la prestación de productos o servicios.

«**CCPA**» se refiere a la Ley de Privacidad del Consumidor de California, modificada por la Ley de Derechos de Privacidad de California u otras leyes o reglamentos de California.

«**Persona Interesada**» hace referencia a la persona a la que se refieren los Datos Personales del Cliente.

«Marco de Privacidad de Datos» se refiere al marco legal entre la UE y los Estados Unidos para las transferencias transfronterizas de Datos Personales entre la Unión Europea y los Estados Unidos e incluye la extensión británica a la UE y los Estados Unidos. DPF y DPF Suiza-Estados Unidos.

«**Leyes de Protección de Datos**» se refiere al Reglamento General de Protección de Datos (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de los Datos Personales y a la libre circulación de dichos datos, y por el que se deroga la Directiva 95/46/CE (y cualquier modificación o sustitución de la misma) o el RGPD de la UE en su forma enmendada e incorporada a la legislación británica en virtud de la Ley de la Unión Europea Británica (retirada) de 2018 y la legislación secundaria aplicable establecida en virtud de esta Ley (y de cualquier modificación o sustitución)) o cualquier otra política de privacidad aplicable legislación que exija una DPA, según proceda (incluida la CCPA).

«**Datos Personales**» hace referencia a toda la información relacionada con un interesado, que incluye, entre otros, el nombre, el número de identificación, los 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 interesado.

«**Proceso**» o «**Procesamiento**» se refiere a cualquier operación o conjunto de operaciones que se lleve a cabo con los Datos Personales del Cliente, ya sea por medios automatizados o no, como la recopilación, el registro, la organización, la estructuración, el almacenamiento, la alteración, la recuperación, la consulta, el uso, la eliminación, la restricción, el acceso, la difusión, la combinación, la copia, la transferencia, la eliminación o la destrucción de los Datos Personales del Cliente.

«**Violación de Seguridad**» hace referencia a una infracción de seguridad confirmada que dé lugar a la destrucción, pérdida, alteración, divulgación o acceso no autorizado accidental o ilegal a los Datos Personales del Cliente transmitidos, almacenados o procesados de otro modo.

«Tercero» hace referencia a una parte que no sea el Cliente o la Empresa.

Los términos «**responsable**», «**procesador**» y «**autoridad supervisora**», tal como se utilizan en esta DPA, tendrán el mismo significado que se les asigna en el RGPD.

Todos los demás términos que no estén definidos sino que estén en mayúscula tendrán el significado establecido en el contrato o en la legislación de privacidad aplicable.

2. Tratamiento de los Datos Personales de los Clientes

2.1 Propósito del Tratamiento. La finalidad del Procesamiento de datos en virtud de esta DPA es proporcionar los productos o servicios de conformidad con el Contrato. En el Apéndice 1 se describen el propósito y los detalles del Procesamiento de los Datos Personales de los Clientes.

2.2 Responsabilidades del Procesador y del Controlador de Datos. Las partes reconocen y aceptan que: (a) La Empresa procesa los Datos Personales de los Clientes en virtud de las Leyes de Protección de Datos; (b) el Cliente es 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 todos los permisos y aprobaciones necesarios para introducir, utilizar, almacenar y procesar los Datos Personales del Cliente a fin de que la Empresa pueda entregar los productos o servicios; y (d) cada parte respetará las obligaciones aplicables de conformidad con Leyes de Protección de Datos con respecto al Procesamiento de Datos Personales del Cliente.

2.3 Leyes Estadounidenses de Protección de Datos. A los efectos de las Leyes de Protección de Datos de los EE. UU. (incluida la CCPA), «controlador de datos» incluye «empresa»; «procesador» incluye «proveedor de servicios»; «Sujeto de Datos» incluye «consumidor» y «Datos Personales» incluye «información personal». La Empresa es un proveedor de servicios y el Cliente es una empresa.

2.4 Instrucciones para los Clientes. El Cliente exige que la Empresa procese sus Datos Personales: (a) de conformidad con el Contrato y cualquier suplemento aplicable; (b) según sea necesario para proporcionar los productos o servicios al Cliente; (c) de conformidad con la ley o los reglamentos aplicables; y (d) para cumplir con otras instrucciones escritas razonables que dé el Cliente cuando dichas instrucciones estén de acuerdo con las condiciones del Contrato. El Cliente se asegurará de que sus instrucciones para el Procesamiento de sus Datos Personales cumplan con las Leyes

de Protección de Datos. Entre las partes, el Cliente es el único responsable de la precisión, la calidad y la legalidad de sus Datos Personales y de la forma en que los obtuvo.

2.5 Cumplimiento por Parte de la Empresa de las Instrucciones del Cliente. La Empresa solo procesará los Datos Personales del Cliente de acuerdo con las instrucciones del Cliente y los tratará como información confidencial. Si la Compañía cree o se entera de que alguna de las instrucciones del Cliente va en contra de las Leyes de Protección de Datos, informará al Cliente en un plazo razonable. La Compañía puede procesar los Datos Personales del Cliente de forma distinta a las instrucciones escritas del Cliente si así lo exige la ley aplicable a la que está sujeta la Empresa. En este caso, la Compañía informará al Cliente de este requisito antes de procesar los Datos Personales del Cliente, a menos que lo prohíba la ley aplicable.

2.6 Tratamiento de la CCPA. En la medida en que el Procesamiento de los Datos Personales por parte de la Empresa esté sujeto a la CCPA, la Empresa certifica que no debe: (a) mantener, utilizar o divulgar los Datos Personales de los Clientes de forma distinta a lo dispuesto en el Contrato, proporcionar los productos o servicios, crear o mejorar la calidad de los productos o servicios, detectar incidentes de seguridad, protegerse contra actividades fraudulentas o ilegales, utilizar subcontratistas de conformidad con esta DPA o según lo autorice la CCPA; o (b) vender o compartir Datos Personales de los Clientes.

3. Subprocesadores

3.1 Designación de los Subcontratistas. Por la presente, el Cliente proporciona una autorización general por escrito que permite a la Compañía utilizar subcontratistas externos para prestar servicios limitados o auxiliares relacionados con el suministro de productos o servicios. El sitio web de la Empresa incluye una lista de los subprocesadores contratados actualmente por la Empresa para realizar actividades de procesamiento específicas relacionadas con los Datos Personales de los Clientes (https://commandalkon.com/sub-processor-list/) y la Empresa actualizará la lista de subprocesadores antes de contratar a un nuevo procesador para que realice un procesamiento específico. El Cliente puede suscribirse para recibir actualizaciones electrónicas cada vez que se modifique la lista de subcontratistas de la Compañía enviando una solicitud de este tipo a privacy@commandalkon.com. El Cliente puede oponerse a cualquier subcontratista comunicando su objeción a la Compañía en un plazo de treinta (30) días a partir de la actualización, y las partes trabajarán de buena fe para resolver la objeción. El Cliente acepta las actividades de subprocesamiento realizadas por los subcontratistas actuales que figuran en el sitio web de la Compañía.

3.2 Seguridad del Subprocesador. Cuando la Compañía subcontrate sus obligaciones, solo lo hará mediante un acuerdo escrito con el subcontratista que imponga obligaciones contractuales que sean al menos equivalentes a las que se imponen a la Compañía en virtud de este apéndice.

3.3 Responsabilidad. Si el subcontratista no cumpla con sus obligaciones de protección de datos en virtud de dicho acuerdo escrito, la Compañía seguirá siendo plenamente responsable ante el Cliente del cumplimiento de las obligaciones del subcontratista en virtud del presente acuerdo.

4. Responsabilidades de Seguridad

4.1 Seguridad Empresarial. La Empresa implementará las medidas técnicas y organizativas adecuadas para proteger los Datos Personales de los Clientes («**Programa de Seguridad de la Información**»), teniendo en cuenta el estado de la técnica, los costes de implementación, la naturaleza, el alcance, el contexto y los objetivos del Procesamiento, así como el riesgo más o menos probable para los derechos y libertades de las personas físicas. La Empresa opera según los siguientes estándares de seguridad: NIST 800-171; AWS CIS.

4.2 Seguridad de los Clientes. El Cliente reconoce que los productos o servicios incluyen ciertas características y funcionalidades que puede optar por utilizar y que afectan a la seguridad de los Datos Personales del Cliente procesados en el contexto de su uso de los productos o servicios. El Cliente es responsable de revisar la información puesta a disposición por la Empresa en relación con la seguridad de sus datos y de determinar de forma independiente si los productos o servicios cumplen con los requisitos y obligaciones legales del Cliente, incluidas sus obligaciones en virtud de la legislación de protección de datos aplicable. El Cliente también es responsable de la configuración correcta de los productos o servicios y del uso de las funcionalidades puestas a disposición por la Compañía a fin de garantizar la seguridad adecuada, dada la naturaleza de los Datos Personales del Cliente procesados en el contexto del uso de los productos o servicios por parte del Cliente. El Cliente es responsable del uso que haga de los productos o servicios y de almacenar cualquier copia de sus Datos Personales fuera de los sistemas de la Empresa o de los subcontratistas de la Empresa, lo que incluye, entre otros, proteger las credenciales, los sistemas y dispositivos de autenticación de cuentas y conservar copias de los Datos Personales del Cliente, si procede.

4.3 Personal de la Empresa. La Empresa debe asegurarse de que su personal responsable del tratamiento de los Datos Personales de los Clientes esté informado de la naturaleza confidencial de los Datos Personales de los Clientes, haya recibido la formación adecuada sobre sus responsabilidades y esté sujeto a las obligaciones de confidencialidad, obligaciones que sobrevivirán al final de la relación de esa persona con la Empresa.

4.4 Pruebas de Seguridad. La Empresa pondrá a prueba, evaluará y evaluará la eficacia del Programa de Seguridad de la Información para garantizar el Procesamiento seguro de los Datos Personales de los Clientes. La Empresa cumplirá con su Programa de Seguridad de la Información y declara y garantiza que su Programa de Seguridad de la Información cumple y cumplirá con la legislación aplicable.

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

5. Derechos de las Personas Afectadas

5.1 Asistencia para Cumplir con las Obligaciones del Cliente. En la medida en que el Cliente, al utilizar o recibir los productos o servicios, no pueda corregir, modificar,

restringir, bloquear o eliminar sus Datos Personales según lo exige la legislación de protección de datos, la Compañía debe responder sin demora a las solicitudes razonables del Cliente para facilitar dichas acciones, en la medida en que la Compañía esté legalmente autorizada y sea capaz de hacerlo. Si la ley lo permite, el Cliente es responsable de todos los costes asociados a la prestación de dicha asistencia por parte de la Compañía.

5.2 Obligaciones de Notificación. En la medida en que lo permita la ley, la Compañía informará inmediatamente al Cliente si recibe una solicitud de acceso, corrección, modificación, eliminación u objeción al Procesamiento de los Datos Personales del Cliente relativos a esa persona. La Compañía no responderá a ninguna solicitud de este tipo relacionada con los Datos Personales del Cliente sin el consentimiento previo por escrito del Cliente, excepto para confirmar que la solicitud se refiere al Cliente. Además, en la medida en que lo permita la ley, la Compañía informará inmediatamente al Cliente si recibe una solicitud de divulgación o correspondencia, una notificación o cualquier otra comunicación relativa a los Datos Personales del Cliente por parte de las fuerzas del orden, de una autoridad competente o de una autoridad de protección de datos competente. La Compañía proporcionará al Cliente la cooperación y la asistencia adecuadas y razonables para tramitar 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 mediante el uso o la recepción de los productos o servicios. Si la ley lo permite, el Cliente es responsable de todos los costes asociados a la prestación de dicha asistencia por parte de la Compañía.

6. Violación de Datos Personales

6.1 Obligaciones de Notificación. Si la Empresa tiene conocimiento de una infracción de seguridad comprobada relacionada con los Datos Personales del Cliente, informará al Cliente lo antes posible y, en cualquier caso, a más tardar setenta y dos (72) horas después de su descubrimiento. Las obligaciones establecidas en esta sección 6 no se aplican a los incidentes causados por el Cliente o el personal del Cliente o los usuarios finales, ni a los intentos o actividades fallidos que no pongan en peligro la seguridad de los Datos Personales del Cliente, incluidos los intentos fallidos de inicio de sesión, los pings, los escaneos de puertos, los ataques de denegación de servicio y otros ataques de red contra firewalls o sistemas de red.

6.2 Modo de Notificación. La notificación de las infracciones 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 mantener la información de contacto precisa en los sistemas de soporte de la Empresa en todo momento. El Cliente es el único responsable de cumplir con los requisitos de notificación aplicables al Cliente y de cualquier obligación de notificar a un tercero en relación con una violación de la seguridad de los Datos Personales.

6.3 Contenido de la Notificación. Cuando se requiera la notificación, como mínimo, debería:

6.3.1 describa la naturaleza de la infracción de seguridad, las categorías y el número de personas afectadas y las categorías y el número de registros de Datos Personales en cuestión;

6.3.2 comunicar el nombre y los datos de contacto del contacto de la Empresa correspondiente, del que se puede obtener más información;

6.3.3 describa las posibles consecuencias de la infracción de seguridad; y

6.3.4 Describa las medidas adoptadas o propuestas para abordar esta infracción de seguridad.

7. Eliminación o Devolución de los Datos Personales de los Clientes

7.1 Retirar o Devolver. Sujeto a la sección 7.3, la Empresa se compromete a eliminar de forma inmediata y en cualquier caso los Datos Personales del Cliente en un plazo de treinta (30) días a partir de la fecha de interrupción de cualquier servicio que implique el Procesamiento de Datos Personales del Cliente (la «**Fecha de Rescisión**»), a Eliminar de forma segura los Datos Personales del Cliente o, previa solicitud por escrito del Cliente en el momento oportuno, a devolver una copia completa de todos los Personales del Cliente mediante transferencia segura de archivos en el formato razonablemente solicitado por el Cliente.

7.2 Definición de Supresión. Para obtener más información, «**Eliminar**» significa eliminar o borrar los Datos Personales del Cliente para que no se puedan recuperar ni reconstruir.

7.3 Registros. La Empresa puede conservar los Datos Personales de los Clientes en la medida en que lo exijan las leyes aplicables o de conformidad con el programa de conservación de documentos de la Empresa, siempre que la Empresa garantice la confidencialidad de todos esos Datos Personales de los Clientes.

8. Derechos de Auditoría

8.1 Derechos de Auditoría. No más de una vez al año, el Cliente puede contratar a un tercero de mutuo acuerdo para que audite la Compañía con el único fin de cumplir con sus requisitos de auditoría de conformidad con el artículo 28, sección 3 (h) del GDPR. 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, en el que se describa el alcance, la duración y la fecha de inicio propuestos de la auditoría. Las solicitudes de auditoría deben enviarse a privacy@commandalkon.com. El auditor debe firmar un acuerdo de confidencialidad por escrito aceptable para la Compañía antes de realizar la auditoría. La auditoría debe realizarse durante el horario laboral habitual, de acuerdo con las políticas de la Empresa, y no debe interferir irrazonablemente con las actividades comerciales de la Empresa. Todas las auditorías corren por cuenta y por cuenta del Cliente. La Compañía cooperará con cualquier Cliente o solicitud de auditoría de una autoridad reguladora o supervisora competente para comprobar el cumplimiento por parte de la Compañía de sus obligaciones en virtud de la presente DPA poniendo a disposición, con sujeción a las obligaciones de confidencialidad, informes de auditoría de terceros, si procede, y/o descripciones de los controles de seguridad y otra información que el Cliente solicite razonablemente en relación con las prácticas y políticas de seguridad de la Empresa.

8.2 Asistencia de Cumplimiento. Dada la naturaleza del Procesamiento y la información puesta a disposición de la Empresa, la Compañía prestará la cooperación y la asistencia adecuadas y razonables al Cliente con respecto a 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 Compañía pueda, con sujeción a la sección 9.2, almacenar y procesar los Datos Personales de los Clientes en los Estados Unidos de América y en cualquier otro país en el que la Compañía o uno de sus subcontratistas tenga instalaciones o procese los Datos Personales de otro modo. Cualquier transferencia de este tipo se regirá principalmente por la certificación del Marco de Privacidad de Datos de la Compañía o, si no, por las cláusulas contractuales estándar interafiliadas de la Compañía. La Compañía no transferirá ni hará que los Datos Personales del Cliente se transfieran de una jurisdicción a otra, excepto de conformidad con la ley aplicable, y no exigirá al Cliente que infrinja ninguna ley de protección de datos.

9.2 Cláusulas Contractuales Estándar. En la medida y únicamente en la medida en que la Empresa procese los Datos Personales de los Clientes del Espacio Económico Europeo y se exijan cláusulas contractuales estándar, se aplica el módulo 2 de las cláusulas contractuales estándar y se incorpora al presente documento. A los efectos de las cláusulas contractuales tipo, el Cliente es el «exportador de datos» y la Empresa es la «importadora de datos».

9.3 Apéndice Británico a las Cláusulas Contractuales Estándar de la UE. En la medida y únicamente en la medida en que la Empresa procese los Datos Personales de los Clientes del Reino Unido y cuando se requieran cláusulas contractuales estándar, las partes acuerdan que la adenda británica se aplicará a los Datos Personales transferidos a través de los productos o servicios desde el Reino Unido, directamente o mediante transferencia posterior, a un país o destinatario fuera del Reino Unido que la autoridad reguladora u organismo gubernamental británico correspondiente al Reino Unido no reconozca que proporciona un nivel adecuado de protección para el personal datos.

9.4 FADP Suizo. En la medida y únicamente en la medida en que la Empresa procese los Datos Personales de los Clientes desde Suiza, se aplican 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 GDPR de la UE: (a) el término «Estado miembro» no debe interpretarse de tal manera que excluya a los interesados en Suiza de la posibilidad de hacer valer sus derechos en su lugar de residencia habitual (Suiza) de conformidad con la cláusula 18 (c) de las cláusulas contractuales estándar; (b) en la medida en que el las transferencias de datos subyacentes a las cláusulas contractuales tipo están sujetas exclusivamente a la FADP, las referencias al GDPR de la UE deben considerarse referencias a la FADP; (c) en la medida en que las transferencias de datos subyacentes a las cláusulas contractuales tipo estén sujetas tanto a la FADP como al GDPR de la UE, las referencias al GDPR de la UE deben considerarse referencias a la FADP en la medida en que las transferencias de datos están sujetas a la FADP; y (d) hasta entra en vigor la ley suiza de protección de datos (rev.) (FADP), y las disposiciones de las cláusulas

contractuales estándar también proteger los Datos Personales de los Clientes en la medida en que estas disposiciones les sean aplicables en virtud de la legislación suiza.

9.5 Medidas Adicionales. Además de las cláusulas contractuales estándar, si la Compañía se entera de que una autoridad gubernamental (incluidas las fuerzas del orden) desea acceder a algunos o todos los Datos Personales de los Clientes procesados por la Compañía, ya sea de forma voluntaria u obligatoria, para fines relacionados con la inteligencia de seguridad nacional, a menos que lo prohíba la ley o exija lo contrario, la Compañía: 1) informará inmediatamente al Cliente al que se aplican los Datos Personales; 2) informará a la autoridad gubernamental correspondiente no ha sido autorizado a revelar al Cliente Datos Personales y, a menos que lo prohíba la ley, debe informar inmediatamente al Cliente al que se aplican los Datos Personales del Cliente; 3) informar a las autoridades gubernamentales de que deben dirigir todas las solicitudes o solicitudes directamente al Cliente al que se aplican los Datos Personales del Cliente; y 4) no proporcionar acceso a los Datos Personales del Cliente antes de haber obtenido la autorización por escrito del Cliente correspondiente o de estar legalmente obligado a hacerlo. Si la ley lo exige, la Compañía hará todos los esfuerzos legales y razonables para impugnar esta prohibición o restricción. Si la Empresa está obligada a proporcionar los Datos Personales del Cliente, solo los divulgará en la medida en que lo exija la ley, de conformidad con el procedimiento legal aplicable.

9.6 Ley de Vigilancia de la Inteligencia Extranjera. La Corporación aún no había recibido ninguna orden en virtud del artículo 702 de la Ley de Vigilancia de la Inteligencia Extranjera de los Estados Unidos, codificada en 50 U.S.C. § 1881a («Sección 702 de la FISA»). Ningún tribunal consideró que la Compañía fuera el tipo de entidad elegible para recibir el tratamiento en virtud de la sección 702 de la FISA. La Empresa no es el tipo de proveedor que reúne los requisitos para la recogida inicial (recogida «masiva») según la sección 702 de la FISA, tal como se describe en la decisión *Schrems* II.

9.7 Prioridad de Transferencia. Si los servicios están cubiertos por varios mecanismos de transferencia, la transferencia de los Datos Personales de los Clientes estará sujeta a un único mecanismo de transferencia de conformidad con el siguiente orden de prioridad: (i) certificación del Marco de Privacidad de Datos corporativos; (ii) cláusulas contractuales tipo de la UE (cuando lo exija la ley de protección de datos aplicable).

10. Duración y Rescisión

Duración de la DPA. Este DPA entrará en vigor en la fecha en que el Contrato se ejecute en su totalidad y, independientemente del vencimiento del plazo de cualquier suscripción adquirida, permanecerá en vigor hasta que se eliminen todos los Datos Personales de los Clientes, tal como se describe en este DPA.

11. Incumplimiento; Recursos; Partes

11.1 Limitación de Responsabilidad. La responsabilidad de la Empresa por el incumplimiento de sus obligaciones en virtud de la presente DPA está sujeta a las disposiciones de limitación de responsabilidad del Contrato.

11.2 Partes de esta DPA. Nada de lo dispuesto en la DPA confiere beneficios o derechos a ninguna persona o entidad que no sean las partes de esta DPA.

12. Condiciones Generales

Ley aplicable y jurisdicción

12.1 Este DPA se revisará un año después de su fecha de publicación y tres años después, o antes si procede.

12.2 A menos que lo exijan las cláusulas contractuales estándar:

12.2.1 las partes de esta adenda se someten a la elección de jurisdicción establecida en el Contrato con respecto a cualquier disputa o reclamación que surja de esta adenda, incluidas las disputas relacionadas con su existencia, validez o rescisión; y

12.2.2 este apéndice y todas las obligaciones extracontractuales o de otro tipo que surjan o estén relacionadas con él se rigen por las leyes del país o territorio especificados a tal efecto en el Contrato.

Orden de prioridad

12.3 En caso de conflicto o incoherencia entre este apéndice y las cláusulas contractuales estándar, cuando se exijan las cláusulas contractuales estándar, prevalecerán las cláusulas contractuales estándar.

12.4 Sin perjuicio de lo dispuesto en la sección 12.2, con respecto al objeto de esta adenda, en caso de incoherencia entre las disposiciones de esta Adenda y cualquier otro acuerdo entre las Partes, incluido el Contrato e incluidos (a menos que se acuerde expresamente lo contrario por escrito y firmados en nombre de las Partes) los acuerdos celebrados o que supuestamente se hayan celebrado después de la fecha de la presente Adenda, prevalecerán las disposiciones de esta Adenda.

Cambios en las Leyes de Protección de Datos

12.5 El Cliente puede:

12.5.1 notificando por escrito a la Compañía con al menos treinta (30) días naturales de vez en cuando, proponga cualquier cambio en las cláusulas contractuales estándar que sea necesario como resultado de una modificación o decisión de una autoridad competente en virtud de esta ley de protección de datos; y

12.5.2 proponer cualquier otra variante de este apéndice que el Cliente considere razonablemente necesaria para cumplir con los requisitos de cualquier ley de protección de datos.

12.6 Si el Cliente lo notifica de conformidad con la sección 12.5, las partes analizarán sin demora las variantes propuestas y negociarán de buena fe con el fin de acordar e implementar estas variantes u otras variantes diseñadas para cumplir los requisitos

identificados en la notificación del Cliente tan pronto como sea razonablemente posible.

Compensación

12.7 Si alguna disposición de este apéndice no es válida o no se puede hacer cumplir, el resto de este apéndice seguirá siendo válida y estará en vigor. La disposición no válida o inaplicable debe: (i) modificarse según sea necesario para garantizar su validez y aplicabilidad, preservando al máximo las intenciones de las partes o, si esto no es posible; (ii) interpretarse de manera que la parte no válida o inaplicable nunca figurara en ella.

Apéndice I: Detalles del Procesamiento de Datos

Exportador de Datos (Controlador de Datos): Cliente tal como se identifica en el Contrato.

Importador de Datos (Procesador): Empresa tal como se identifica en el Contrato.

Finalidad: La finalidad del tratamiento de los datos en virtud de esta DPA se refiere a los Datos Personales de los Clientes.

Duración del Procesamiento: la duración del Contrato más el período hasta que la Compañía elimine todos los Datos Personales de los Clientes de conformidad con esta DPA.

Propósito: El propósito del Procesamiento de datos es proporcionar productos o servicios al Cliente.

Naturaleza del Procesamiento: La naturaleza del Procesamiento de datos está destinada a la prestación de los productos o servicios descritos en el Contrato.

Categorías de Sujetos de Datos: empleados de los Clientes y empleados de las filiales, Clientes y socios comerciales del cliente.

Tipos de Datos Personales: el Cliente puede subir, enviar o proporcionar ciertos Datos Personales relacionados con productos o servicios, cuyo alcance generalmente determina y controla el Cliente a su entera discreción y pueden incluir información de contacto; información sobre las interacciones con el sitio web, los productos y los servicios; direcciones; información de geolocalización; direcciones de correo electrónico; nombres; sexo; título; números de teléfono; número de carné de conducir; firma; número de empleado; tarifa salarial; nombre de usuario; contraseña; información sobre el desempeño; cualificaciones y restricciones; información del dispositivo.

Datos Confidenciales Transferidos: ninguno.

Frecuencia de Transferencia: continua según sea necesario para el suministro de productos o servicios.

Transferencias a Subcontratistas: Como se describe en la lista de subprocesadores de la Compañía disponible en https://commandalkon.com/sub-processor-list/.

Autoridad de Control Competente: de conformidad con las Leyes de Protección de Datos aplicables o, por orden de entrada en vigor, 1) de conformidad con las condiciones del Aontrato o 2) Autoridad holandesa de Protección de Datos.

Retención: de conformidad con el Contrato 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 de la DPA. Hay información adicional disponible a pedido.