ADENDA DE PROCESAMIENTO DE DATOS DE COMMAND ALKON INCORPORATED

Actualizado: 07/21/22

Esta adenda de procesamiento de datos («**APD**») forma parte del *Acuerdo Principal de Licencia y Servicios* («**Acuerdo**») entre: (i) Cliente (identificado en la línea de la firma inferior) y sus filiales en el EEE **(**«**Cliente**»**)**; y (ii) Command Alkon Incorporated y sus filiales («**Empresa**»).

Teniendo en cuenta el Reglamento General de Protección de Datos («RGPD») aplicable, esta Adenda 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 el RGPD.

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

1. Definiciones

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

«**Interesado**» se refiere a la persona física a la que se refieren los Datos Personales del Cliente.

«**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 datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (y cualquier modificación o sustitución de la misma), a la Ley Federal de Protección de Datos de Suiza de 19 de junio de 1992 (y cualquier modificación o sustitución de la misma), o al RGPD de la UE modificado e incorporado a la legislación del Reino Unido en virtud de la Ley de la Unión Europea (Retirada) del Reino Unido de 2018 y a la legislación secundaria aplicable elaborada en virtud de dicha Ley (y cualquier modificación o sustitución de la misma), en función de cuál sea aplicable

«**Datos personales**» se refiere a cualquier información relacionada con un Interesado, entre otros, nombre, número de identificación, datos de ubicación, identificador en línea o uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social del Interesado.

«**Escudo de privacidad**» se refiere al marco legal del Escudo de Privacidad UE-EE. UU. y al marco legal del Escudo de Privacidad Suiza-EE. UU. Aunque ambos marcos son actualmente inoperantes, la empresa continúa adhiriéndose a sus requisitos, y este término se aplicará a cualquier versión renovada y aprobada del acuerdo del Escudo de Privacidad entre los Estados Unidos y el Espacio Económico Europeo («EEE»).

«**Procesamiento**» o «**Tratamiento**» se refiere a cualquier operación o conjunto de operaciones que se realicen sobre los Datos Personales del Cliente, ya sea por medios

automatizados o no, como la recogida, registro, organización, estructuración, almacenamiento, alteración, recuperación, consulta, uso, divulgación, eliminación, restricción, acceso, difusión, combinación, adaptación, copia, transferencia, borrado y/o destrucción de los Datos Personales del Cliente.

«**Violación de la seguridad**» se refiere a una violación de la seguridad que provoque la destrucción accidental o ilegal, la pérdida, la alteración, la divulgación no autorizada o el acceso a los Datos Personales del Cliente transmitidos, almacenados o tratados de otro modo.

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

Los términos «**responsable del tratamiento**», «**encargado del tratamiento**» y «**autoridad de control**» tal como se utilizan en esta APD tendrán el significado que se les atribuye en el RGPD.

Todos los demás términos no definidos pero con mayúsculas tendrán el significado establecido en el Acuerdo.

2. Tratamiento de los datos personales de los clientes

2.1 Finalidad del tratamiento de los datos personales. La finalidad del tratamiento de datos en virtud del presente APD es la prestación de los Productos y/o Servicios de conformidad con el Acuerdo. En el Anexo 1 se describe el objeto y los detalles del tratamiento de los datos personales de los clientes.

2.2 Responsabilidades del encargado 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 bajo las Leyes de Protección de Datos; (b) el Cliente es un responsable de los Datos Personales del Cliente bajo las Leyes de Protección de Datos; y (c) cada parte cumplirá con las obligaciones aplicables a ella bajo las Leyes de Protección de Datos respecto al Tratamiento de los Datos Personales del Cliente.

2.3 Instrucciones para el cliente. El Cliente encarga a la Empresa el Tratamiento de los Datos Personales del Cliente: (a) de acuerdo con el Acuerdo y cualquier Complemento 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 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, la calidad y la legalidad de los Datos Personales del Cliente y de los medios por los que el Cliente ha obtenido los Datos Personales del Cliente.

2.4 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 seguir las instrucciones escritas del Cliente si así lo exige la legislación aplicable a la que está sujeta la Empresa. En esta situación, la Empresa informará al Cliente de dicho requisito antes de que la Empresa trate los Datos Personales del Cliente, a menos que lo prohíba la legislación aplicable.

3. Subencargados del tratamiento

3.1 Designación de subencargados. El cliente autoriza por escrito a la Empresa a contratar a terceros subencargados para que presten servicios limitados o auxiliares en relación con el suministro de productos y/o servicios. En el sitio web de la Empresa se enumeran los subencargados que actualmente son contratados por la Empresa para llevar a cabo actividades de tratamiento específicas relacionadas con los Datos Personales del Cliente y la Empresa actualizará la lista de subencargados antes de contratar a cualquier nuevo subencargado para llevar a cabo un tratamiento específico. El Cliente puede inscribirse para recibir actualizaciones electrónicas cada vez que se modifique la lista de subencargados de la Empresa. El Cliente puede oponerse a cualquier subencargado comunicando dicha objeción a la Empresa en un plazo de treinta (30) días a partir de una actualización, y las partes trabajarán de buena fe para resolver la objeción. El Cliente acepta las actividades de subtratamiento por parte de los subencargados actuales que figuran en el sitio web de la Empresa.

3.2 Seguridad del subencargado. Cuando la Empresa subcontrate sus obligaciones, lo hará únicamente mediante un acuerdo escrito con el subencargado que imponga obligaciones contractuales que sean al menos equivalentes a las obligaciones impuestas a la Empresa en virtud de la presente Adenda.

3.3 Responsabilidad. Si el subencargado no cumple con 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 en virtud de dicho acuerdo.

4. Seguridad y Evaluaciones de Impacto sobre la Privacidad

4.1 Seguridad de la Empresa. La Empresa aplicará 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 las finalidades del Tratamiento, así como el riesgo de probabilidad y gravedad variables para los derechos y libertades de las personas físicas. Las medidas técnicas y organizativas actuales de la Empresa se enumeran en el Anexo II de las Cláusulas Contractuales Estándar (adjunto) y la Empresa se rige por las siguientes normas 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 utilizar y que afectan a la seguridad de los Datos Personales del Cliente tratados para el uso de los productos y/o servicios por parte del Cliente. El Cliente es responsable de revisar la información que la Empresa pone a su disposición en relación con la seguridad de sus datos y de determinar de forma independiente si los productos y/o servicios cumplen con los requisitos y obligaciones legales del Cliente, incluidas sus obligaciones en

virtud de la Ley de Protección de Datos aplicable. Además, el Cliente es responsable de configurar adecuadamente los productos y/o servicios y de utilizar las características y funcionalidades puestas a disposición por la Empresa para mantener la seguridad apropiada 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 de la Empresa, entre otros, la seguridad de las credenciales de autentificación de la cuenta, los sistemas y los dispositivos, y la conservación de las copias de sus Datos Personales del Cliente según corresponda.

4.3 Personal de la empresa. La Empresa se asegurará de que el personal que participe en el tratamiento de los Datos Personales del Cliente sea informado de la naturaleza confidencial de los Datos Personales del Cliente y esté sujeto a obligaciones de confidencialidad, obligaciones que continuarán tras la finalización del compromiso de ese individuo con la Empresa.

4.4 Pruebas de seguridad. La Empresa probará, valorará y evaluará la eficacia del Programa de Seguridad de la Información para garantizar el Tratamiento seguro de los Datos Personales del Cliente. 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 Empresa adoptará medidas razonables para cooperar y dar asistencia al Cliente en la realización de evaluaciones de impacto y consultas relacionadas con cualquier autoridad de supervisión, si el Cliente está obligado a realizar dichas evaluaciones de impacto en virtud de las Leyes de Protección de Datos.

5. Derechos del Interesado

5.1 Asistencia en 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 tal y como exigen las Leyes de Protección de Datos, la Empresa cumplirá con prontitud las solicitudes razonables del Cliente para facilitar dichas acciones en la medida en que la Empresa esté legalmente autorizada y pueda hacerlo. Si la ley lo permite, el Cliente será responsable de cualquier coste derivado de la prestación de dicha asistencia por parte de la Empresa.

5.2 Obligación de Notificación. La Empresa, en la medida en que lo permita la ley, notificará de inmediato al Cliente si recibe una solicitud de un Interesado para acceder, corregir, modificar, eliminar u objetar el Tratamiento de los Datos Personales del Cliente relativos a dicha persona. La Empresa no responderá a ninguna de estas solicitudes de los Interesados relacionadas 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, la Empresa, en la medida en que lo permita la ley, notificará inmediatamente al Cliente si recibe una solicitud de divulgación o correspondencia, notificación u otra comunicación relativa a 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 proporcionará al Cliente la cooperación y asistencia adecuadas y razonables en relación con la gestión de cualquier solicitud de este tipo, en la medida en que esté legalmente permitido 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 la ley lo permite, 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 Obligación de Notificación. En caso de que la Empresa tenga conocimiento de una Violación de la Seguridad verificada, la Empresa notificará al Cliente la Violación de la Seguridad sin demora injustificada y, en cualquier caso, no más tarde de setenta y dos (72) horas desde su detección. Las obligaciones del presente Apartado 6 no se aplican a los incidentes causados por el Cliente o por el personal o los usuarios finales del Cliente, ni a los intentos o actividades infructuosos que no pongan en peligro la seguridad de los Datos Personales del Cliente, incluidos los intentos infructuosos de inicio de sesión, los pings, los escaneos de puertos, los ataques de denegación de servicio y otros ataques de red a los cortafuegos o a los sistemas en red.

6.2 Modalidad de Notificación. La Notificación de las Violaciones de la Seguridad, si las hubiera, se hará a la persona de contacto del Cliente del RGPD por correo electrónico o por teléfono. Es responsabilidad exclusiva del Cliente asegurarse de que mantiene una información de contacto precisa en los sistemas de soporte de la Empresa en todo momento.

6.3 Contenido de la Notificación. Cuando se requiera una notificación, ésta deberá, como mínimo:

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 de la Empresa de la que se puede obtener más información;

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

6.3.4 describir las medidas adoptadas o que se proponen adoptar para hacer frente a la Violación de la Seguridad.

7. Supresión o Devolución de los Datos Personales del Cliente

7.1 Supresión o Devolución. Sin perjuicio de lo dispuesto en el apartado 7.3, la Empresa se compromete a que, en un plazo de treinta (30) días a partir de la fecha de cese de cualquier servicio que implique el Tratamiento de los Datos Personales del Cliente (la «**Fecha de cese**»), eliminar de forma segura los Datos Personales del Cliente o, si el Cliente lo solicita oportunamente por escrito, devolverle una copia completa de todos

y cada uno de los Datos Personales del Cliente mediante una transferencia segura de archivos en el formato que el Cliente solicite razonablemente.

7.2 Definición de Eliminación. Como aclaración, «**Eliminar**» se refiere a eliminar o borrar los Datos Personales de manera que no puedan ser recuperados o reconstruidos.

7.3 Registros. La Empresa podrá conservar los Datos Personales del Cliente en la medida en que lo exija la Legislación Aplicable o lo disponga la programación de conservación de documentos de la Empresa, siempre que ésta garantice la confidencialidad de todos esos Datos Personales del Cliente.

8. Derechos de Auditoría

8.1 Derechos de Auditoría. Como máximo una vez al año, el Cliente podrá contratar a un tercero de mutuo acuerdo para que audite a la Empresa con el único fin de cumplir con sus requisitos de auditoría de conformidad con el artículo 28, apartado 3, letra (h) del RGPD. Para solicitar una auditoría, el Cliente debe presentar un plan de auditoría detallado con al menos cuatro (4) semanas de antelación a la fecha de auditoría propuesta, en el que se describa el alcance, la duración y la fecha de inicio de la misma. Las solicitudes de auditoría deben enviarse a privacy@commandalkon.com. El auditor debe firmar un acuerdo de confidencialidad por escrito aceptable para la Empresa antes de realizar la auditoría. La auditoría debe realizarse durante el horario de trabajo habitual, de acuerdo con las políticas de la Empresa, y no puede interferir injustificadamente con las actividades comerciales de la misma. Todas las auditorías correrán a cargo del Cliente. La Empresa cooperará con cualquier Cliente o con cualquier solicitud de auditoría de las autoridades reguladoras o supervisoras competentes para verificar el cumplimiento de la Empresa con sus obligaciones en virtud de este APD, poniendo a su disposición, con sujeción a las obligaciones de no divulgación, informes de auditoría de terceros, cuando estén disponibles, descripciones de los controles de seguridad y otra información razonablemente solicitada por el Cliente en relación con las prácticas y políticas de seguridad de la Empresa.

8.2 Asistencia para el Cumplimiento. Al tener en cuenta la naturaleza del Tratamiento y la información disponible para la Empresa, esta proporcionará una cooperación y asistencia razonables y adecuadas 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 procesar 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 mantenga instalaciones o procese de otro modo los Datos Personales. Dichas transferencias se regirán por las Cláusulas Contractuales Estándar de la Empresa o por la certificación del Escudo de Privacidad de la Empresa (en caso de que se restablezca). La Empresa no transferirá, ni hará que se transfiera, ningún Dato Personal del Cliente de una jurisdicción a otra a menos que sea de conformidad con la legislación aplicable y no hará que el Cliente infrinja ninguna Ley de Protección de Datos.

9.2 Cláusulas Contractuales Estándar. En la medida, y solo en la medida, en que la Empresa trate Datos Personales del Cliente procedentes del Espacio Económico Europeo, Suiza o el Reino Unido y se requieran Cláusulas Contractuales Estándar, se aplicarán las Cláusulas Contractuales Estándar aplicables (EEE o Reino Unido) y se incorporan en este documento. A efectos de las Cláusulas Contractuales Estándar, el Cliente es el «exportador de datos» y la Empresa es el «importador de datos». La Empresa cuenta con las Cláusulas Contractuales Estándar 2021 entre las filiales de la Empresa y ha mantenido la autocertificación al Escudo de Privacidad (en caso de que se restablezca) a efectos de las transferencias de datos a los Estados Unidos de América.

9.3 Cláusulas Contractuales Estándar del Reino Unido. Las partes acuerdan que las Cláusulas Contractuales Estándar del Reino Unido se aplicarán a los datos personales que se transfieran a través de los productos y/o servicios desde el Reino Unido, ya sea directamente o a través de una transferencia posterior, a cualquier país o destinatario fuera del Reino Unido que no esté reconocido por la autoridad de control competente del Reino Unido o por el organismo gubernamental del Reino Unido como proveedor de un nivel adecuado de protección de los datos personales. En el caso de las transferencias de datos desde el Reino Unido que estén sujetas a las Cláusulas Contractuales Estándar del Reino Unido, las Cláusulas Contractuales Estándar del Reino Unido se considerarán firmadas (e incorporadas a esta Adenda con esta referencia).

9.4 Medidas Complementarias. Como complemento a las Cláusulas Contractuales Estándar, si la Empresa tiene conocimiento de que cualquier autoridad gubernamental (incluidas las fuerzas de seguridad) 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, entonces, a menos que esté legalmente prohibido o bajo una obligación legal que requiera lo contrario, la Empresa: 1) notificar inmediatamente al Cliente al que se aplican los datos personales; 2) informar a la autoridad gubernamental pertinente que no ha sido autorizada a revelar los Datos Personales del Cliente y, a menos que esté legalmente prohibido, deberá notificar inmediatamente al Cliente al que 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 sea autorizado por escrito por el Cliente al que se aplican los Datos Personales del Cliente o hasta que sea obligado legalmente a hacerlo. Si se ve obligada legalmente a hacerlo, la Empresa hará esfuerzos razonables y legales para impugnar dicha prohibición u obligación. Si la Empresa se ve obligada a presentar los Datos Personales del Cliente, ésta solo revelará los Datos Personales del Cliente en la medida en que se le exija legalmente de acuerdo con el proceso legal aplicable.

9.5 Precedencia de 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) Cláusulas Contractuales Estándar de la UE (cuando lo exija la Ley de Protección de Datos aplicable); (ii) Autocertificación del Escudo de Privacidad (si se restablece).

10. Vigencia y finalización

Vigencia del APD. Este APD entrará en vigor en la fecha en que se ejecute por completo y, a pesar de la expiración del plazo de cualquier suscripción adquirida, permanecerá en vigor hasta que se eliminen todos los Datos Personales del Cliente, tal y como se describe en este APD, y expirará automáticamente.

11. Incumplimiento; Recursos; Partes

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

11.2 Partes de este APD. Nada de lo dispuesto en el APD conferirá beneficios o derechos a ninguna persona o entidad distinta de las partes de este APD.

12. Condiciones generales

Derecho aplicable y jurisdicción

12.1 Este APD se revisará un año después de la fecha de emisión y tres años después, o antes si procede.

12.2 Salvo que lo requieran las Cláusulas Contractuales Estándar:

12.2.1 las partes de esta Adenda se someten a la elección de la jurisdicción estipulada en el Acuerdo con respecto a cualquier disputa o reclamación que surja en virtud de la misma, incluidas las disputas sobre su existencia, validez o terminación; y

12.2.2 esta Adenda y todas las obligaciones extracontractuales o de otro tipo que se deriven de ella o estén relacionadas con ella se rigen por las leyes del país o territorio estipulado a tal efecto en el Acuerdo.

Orden de Precedencia

12.3 En caso de conflicto o incoherencia entre la presente Adenda y las Cláusulas Contractuales Estándar, cuando se requieran las Cláusulas Contractuales Estándar, prevalecerán las Cláusulas Contractuales Estándar.

12.4 Sujeto a la sección 12.2, en lo que respecta al objeto de esta Adenda, en caso de incoherencias entre las disposiciones de esta Adenda y cualquier otro acuerdo entre las partes, incluido el Contrato e incluso (salvo acuerdo explícito en contrario, firmado por escrito en nombre de las partes) los acuerdos celebrados o que se pretendan celebrar después de la fecha de esta Adenda, prevalecerán las disposiciones de esta Adenda.

Cambios en las Leyes de Protección de Datos

12.5 El Cliente puede:

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

12.5.2 proponer cualquier otra variación de esta Adenda que el Cliente considere razonablemente necesaria para abordar los requisitos de cualquier Ley de Protección de Datos.

12.6 Si el Cliente notifica en virtud de la sección 12.5, las partes discutirán sin demora las variaciones propuestas y negociarán de buena fe con el fin de acordar y aplicar dichas variaciones o variaciones alternativas diseñadas para abordar los requisitos identificados en la notificación del Cliente tan pronto como sea razonablemente factible.

Indemnización

12.7 Si alguna de las disposiciones de esta Adenda fuera inválida o inaplicable, el resto de esta Adenda seguirá siendo válida y vigente. La disposición inválida o inaplicable será: (i) modificada en la medida necesaria para asegurar su validez y ejecutabilidad, preservando al máximo las intenciones de las partes o, si esto no es posible; (ii) interpretada como si la parte inválida o inaplicable nunca hubiera estado contenida en ella.

ANEXO I DE LAS CLÁUSULAS CONTRACTUALES ESTÁNDAR

A. LISTA DE PARTES

Exportador(es) de datos[1]**:** [*Identidad y datos de contacto del exportador(es) de datos y, en su caso, de su responsable de la protección de datos y/o representante en la Unión Europea]*

Nombre:

Dirección:

Nombre de la persona de contacto, cargo y datos de contacto:

Actividades relacionadas con los datos transferidos en virtud de estas Cláusulas:

Firma y fecha:

Función: Responsable del tratamiento

Importador(es) de datos: [*Identidad y datos de contacto del/los importador(es) de datos, incluida cualquier persona de contacto responsable de la protección de datos]*

Nombre: Command Alkon Incorporated

Dirección: 1800 Industrial Park Drive, Suite 400, Birmingham, Alabama 35243 EE. UU.

Nombre de la persona de contacto, cargo y datos de contacto: David R. Burkholder, Consejero General Asociado y Jefe del Departamento de Privacidad, dburkholder@commandalkon.com, 1-205-263-5524 ext. 2837

Actividades relacionadas con los datos transferidos en virtud de estas Cláusulas:

Jefe del Departamento de Privacidad a efectos de cumplimiento

Firma y fecha:

Función: Encargado del tratamiento

B. DESCRIPCIÓN DE LA TRANSFERENCIA

Categorías de interesados cuyos datos personales se transfieren

[1] Si no se cumplimenta esta sección, el Exportador de Datos será la entidad identificada en el Acuerdo Principal de Licencia y Servicios y los documentos asociados.

Empleados del Cliente; clientes del Cliente; empleados de empresas afiliadas al Cliente.

Categorías de datos personales transferidos

Información de contacto; información de 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; tasa de pago; nombre de usuario; contraseña; información sobre el rendimiento; cualificaciones y restricciones.

Datos sensibles transferidos (si procede) y restricciones o salvaguardias aplicadas que tengan plenamente en cuenta la naturaleza de los datos y los riesgos implicados, como, por ejemplo, la limitación estricta de la finalidad, las restricciones de acceso (incluido el acceso solo para el personal que haya seguido una formación especializada), el mantenimiento de un registro de acceso a los datos, las restricciones para las transferencias ulteriores o las medidas de seguridad adicionales

No se transfieren datos sensibles conforme al RGPD.

La frecuencia de la transferencia (por ejemplo, si los datos se transfieren de forma puntual o continua).

Transferencia continua de datos a medida que el producto/plataforma es utilizado por los usuarios finales.

Naturaleza del tratamiento

Según sea necesario para el suministro del producto/servicio en virtud del Acuerdo y según las instrucciones del Exportador.

Finalidad(es) de la transferencia de datos y del tratamiento posterior

Según sea necesario para el suministro del producto/servicio o como soporte del mismo.

El plazo durante el cual se mantendrán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo

Durante el plazo necesario para suministrar el producto/servicio y en conjunción con la política y el calendario de conservación de datos de la empresa o según lo exija la legislación o la normativa aplicable.

Para las transferencias a (sub)encargados, especificar también el objeto, la naturaleza y la duración del tratamiento

Para el soporte necesario para proporcionar el producto/servicio (por ejemplo, servicios de almacenamiento en la nube) y durante el período necesario para proporcionar el producto/servicio.

C. AUTORIDAD DE CONTROL COMPETENTE

Identificar la(s) autoridad(es) de control competente(s) de acuerdo con la cláusula 13

Autoridad de Protección de Datos de los Países Bajos.

ANEXO II DE LAS CLÁUSULAS CONTRACTUALES ESTÁNDAR

MEDIDAS TÉCNICAS Y ORGANIZATIVAS, INCLUIDAS LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA SEGURIDAD DE LOS DATOS

Descripción de las medidas técnicas y organizativas implementadas por el/los importador(es) de datos (incluidas las certificaciones pertinentes) para garantizar un nivel de seguridad adecuado, teniendo en cuenta la naturaleza, el alcance, el contexto y la finalidad del tratamiento, así como los riesgos para los derechos y las libertades de las personas físicas.

Medidas de seudonimización y cifrado de datos personales **Se implementa el cifrado en tránsito y en reposo**

Medidas para garantizar la confidencialidad, integridad, disponibilidad y resistencia permanentes de los sistemas y servicios de procesamiento **Command Alkon se rige por el marco de seguridad NIST 800-171, así como por los AWS CIS Benchmarks v1.2 y AWS Foundational Best Practices v1.0**

Medidas para garantizar la capacidad de restablecer la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico **Command Alkon realiza copias de seguridad periódicas y utiliza una arquitectura de alta disponibilidad**

Procesos para comprobar, valorar y evaluar periódicamente la eficacia de las medidas técnicas y organizativas con el fin de garantizar la seguridad del tratamiento **Pruebas periódicas automatizadas de vulnerabilidad; pruebas anuales de penetración; auditorías anuales de privacidad y seguridad**

Medidas de identificación y autorización de los usuarios **Autenticación multifactorial; programa sofisticado de contraseñas; limitaciones de permisos; registro**

Medidas de protección de los datos durante la transmisión **Cifrado en tránsito**

Medidas de protección de datos durante el almacenamiento **Cifrado en reposo; controles de acceso lógico; redundancia mediante copias de seguridad y conmutación por error**

Medidas para garantizar la seguridad física de los lugares en los que se tratan los datos personales **Tarjetas/códigos de acceso; registro de visitantes; vídeo de seguridad; agentes de seguridad; formación sobre seguridad/privacidad**

Medidas para garantizar el registro de eventos **Registro establecido y supervisado; el registro se transmite a un servicio gestionado por terceros; alertas de eventos activadas**

Medidas para garantizar la configuración del sistema, incluida la configuración predeterminada **Se hace un seguimiento de todos los estados y cambios de configuración; se aplica el programa de gestión de cambios**

Medidas para la gobernanza y la gestión de la seguridad informática interna **Políticas y procedimientos de seguridad y privacidad; director de seguridad de la información; equipo de operaciones de seguridad específico; director de privacidad; formación en seguridad y privacidad**

Medidas de certificación/garantía de procesos y productos **NIST 800-171; CIS AWS Benchmark v1.2; AWS Foundational Best Practices v1.0**

Medidas para garantizar la minimización de los datos **Los datos procesados son solo por campos introducidos por los usuarios finales, clientes o responsables del tratamiento**

Medidas para garantizar la calidad de los datos **Los datos procesados son introducidos y mantenidos por los usuarios finales, clientes o responsables del tratamiento**

Medidas para garantizar un mantenimiento limitado de los datos **La conservación de datos está controlada por las obligaciones contractuales y la política y programación de conservación de datos**

Medidas para garantizar la responsabilidad **La responsabilidad se aborda a través de un registro supervisado; el registro se alimenta a un servicio gestionado por terceros; las alertas de eventos se activan**

Medidas para permitir la portabilidad de los datos y garantizar su eliminación **La portabilidad de los datos se gestiona caso por caso y la supresión se garantiza mediante obligaciones contractuales y procesos de notificación y confirmación**

Para las transferencias a (sub)encargados, también describir las medidas técnicas y organizativas específicas que debe adoptar el (sub)encargado del tratamiento para poder prestar asistencia al responsable del tratamiento y, en el caso de las transferencias de un encargado a un subencargado, al exportador de datos

Los subencargados que tratan datos personales están sujetos a restricciones contractuales y Adendas de Tratamiento de Datos que exigen el cumplimiento de las Cláusulas Contractuales Estándar cuando así se requiera