DATA PROCESSING ADDENDUM ("DPA") FOR CHS INC. SUPPLIERS CONTROLLER TO PROCESSOR (C2P)

In order to fulfill its obligations under applicable data protection and security regulations, CHS Inc. and its Affiliates, ("CHS") will share certain Personal Data with [Insert name of service provider/supplier] ("Supplier") subject to the terms of this addendum ("Addendum"), and only as necessary for Supplier to perform its obligations under [Insert name of service agreement] (the "Primary Agreement"). Supplier will act as an "agent" for CHS for the limited purposes of using, storing, and otherwise processing this Personal Data. This Addendum may be executed in one or more counterparts, each of which will be deemed an original, but all of which taken together will constitute one and the same agreement.

1. **Definitions.** For the purposes of this Addendum, the following terms shall have the following meanings:
   a. **Affiliate(s):** means any other legal entity that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such entity. The term "control" (including the terms "controlled by" and "under common control with") means the direct or indirect power to direct or cause the direction of the management and policies of an entity, whether through the ownership of voting securities, by contract, or otherwise of more than fifty percent (50%) of the voting securities of an entity.
   b. **"Data Privacy Laws"** means any laws that apply to the Processing of Personal Data by Supplier under the Primary Agreement. This includes laws, regulations, guidelines, requirements, and government issued rules in the U.S. and other jurisdictions, at the international, national, state/provincial, or local levels, currently in effect and as they become effective, including without limitation EU Directive 95/46/EC, the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), the UK Data Protection Act, 2018, the California

ADENDA DE TRATAMIENTO DE DATOS ("DPA") PARA PROVEEDORES DE CHS INC. RESPONSABLE A ENCARGADO DE TRATAMIENTO (C2P)

Para cumplir con sus obligaciones en virtud de la normativa aplicable en materia de protección de datos y seguridad, CHS Inc. y sus Empresas Vinculadas ("CHS") compartirán determinados Datos Personales con [Insertar nombre del proveedor de servicios] ("Proveedor"), de conformidad con los términos de esta Adenda ("Adenda"), y únicamente en la medida necesaria para que el Proveedor cumpla con sus obligaciones en virtud de [Insertar nombre del contrato de servicios] (el "Contrato Principal"). El Proveedor actuará como agente de CHS con el único fin de usar, almacenar y tratar de cualquier otra forma estos Datos Personales. Esta Adenda podrá formalizarse en uno o más ejemplares, cada uno de los cuales se considerará original, pero todos ellos, en conjunto, constituirán un único y mismo contrato.

1. **Definiciones.** Para los fines de esta Adenda, los siguientes términos tendrán los siguientes significados:
   a. **Empresa(s) Vinculada(s):** se refiere a cualquier otra persona jurídica que, directa o indirectamente, a través de uno o más intermediarios, controla, es controlada por o está bajo control común con dicha entidad. El término «control» (incluidos los términos «controlado por» y «bajo control común con») se refiere a la facultad, directa o indirecta, de dirigir o influir en la dirección de la administración y las políticas de una sociedad, ya sea mediante la propiedad de acciones con derecho a voto, por contrato o de otro modo, de más del cincuenta por ciento (50 %) de las acciones con derecho a voto de una sociedad.
   b. **"Leyes de Privacidad de Datos"** significa cualquier ley que se aplique al Tratamiento de Datos Personales por parte del Proveedor en virtud del Contrato Principal. Esto incluye leyes, reglamentaciones, lineamientos, requisitos y normas emitidas por el gobierno en los EE. UU. y otras jurisdicciones, a nivel internacional, nacional, estadual/provincial o local, actualmente en vigor y a medida que entren en vigor, incluyendo, sin limitación, la Directiva 95/46/CE de la UE, el Reglamento General de Protección de Datos (Reglamento (UE) 2016/679) ("RGPD"), la Ley de Protección de Datos

Consumer Privacy Act of 2018 (“CCPA”) as amended by the California Privacy Rights Act of 2020 (“CPRA”), the Virginia Consumer Data Protection Act (“VCDPA”), the Colorado Privacy Act (“CPA”), the New York SHIELD Act, the Federal Law for the Protection of Personal Data held by Private Parties and its regulations (“FDPL”), the Brazilian Data Protection Law No. 13,709/2018 (the “LGPD”), and any applicable data security and/or privacy laws of other jurisdictions as may be amended from time to time.

c. **"Data Subject"** means the individual to whom Personal Data relates.

d. **“Information System”** means computer, communication, and network equipment, systems, and services (voice, data, or otherwise) owned, controlled, or used by CHS, including, but not limited to, the corporate wide area network, the electronic switched network, Inter/intranet gateways, electronic mail, telephony, computer systems, system hardware, drives, electronic media, storage areas, software programs, files, and databases.

e. **“Permitted System”** means a CHS Information System to which CHS or CHS Affiliates expressly grants Supplier access and that is necessary for Supplier to perform its obligations to the CHS.

f. **“Personal Data”** means any information received by the Supplier from CHS, or on the CHS’s behalf, that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household.

g. **“Process” or “Processing**” means any operation or set of operations that is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

del Reino Unido, 2018, la Ley de Privacidad del Consumidor de California de 2018 ("CCPA") modificada por la Ley de Derechos de Privacidad de California de 2020 ("CPRA"), la Ley de Protección de Datos del Consumidor de Virginia ("VCDPA"), la Ley de Privacidad de Colorado ("CPA"), la Ley SHIELD de Nueva York, la Ley Federal de Protección de Datos Personales en Posesión de Particulares y sus reglamentarias ("FDPL"), la Ley de Protección de Datos de Brasil N.º 13.709/2018 (la "LGPD") y cualquier ley de seguridad y/o privacidad de datos aplicable de otras jurisdicciones que pueda modificarse oportunamente.

c. **"Titular de Datos"** significa el individuo al que se refieren los Datos Personales.

d. **“Sistema de información”** significa computadoras, equipos de comunicación y redes, sistemas y servicios (voz, datos o de otro tipo) propiedad de, controlados o utilizados por CHS, incluidos, sin limitación, la red de área amplia corporativa, la red electrónica conmutada, puertas de enlace entre redes e intranets, correo electrónico, telefonía, sistemas informáticos, hardware del sistema, unidades, medios electrónicos, áreas de almacenamiento, programas de software, archivos y bases de datos.

e. **“Sistema permitido”** significa un Sistema de Información de CHS al cual CHS o las Empresas Vinculadas de CHS otorgan expresamente acceso al Proveedor y que es necesario para que el Proveedor cumpla con sus obligaciones con CHS.

f. **“Datos Personales”** significa cualquier información recibida por el Proveedor de CHS, o en nombre de CHS, que identifica, se relaciona con, describe, es razonablemente capaz de asociarse con, o podría razonablemente vincularse, directa o indirectamente, con un individuo o familia en particular.

g. **“Proceso” o “Tratamiento**” significa cualquier operación o conjunto de operaciones que se realice sobre Datos Personales, ya sea por procedimientos automatizados o no, como la recopilación, registro, organización, almacenamiento, adaptación o modificación, recuperación, consulta, utilización, divulgación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o

h. **"Security Incident"** means any unlawful or unauthorized access to any of CHS's Personal Data stored on Supplier's equipment or in Supplier's facilities, or access to equipment or facilities resulting in any unauthorized use, acquisition, Processing, loss, destruction, damage, disclosure, theft, copying, modification, or alteration of CHS Personal Data.

2. Obligations of the Supplier.
The Supplier represents and warrants that:

a. It will Process the Personal Data on behalf of CHS, only for the purpose of fulfilling its obligations under the Primary Agreement(s) or as otherwise instructed in writing by CHS, and in accordance with all applicable Data Privacy Laws, and the terms of this Addendum, and will refrain from Processing Personal Data for purposes other than as instructed by CHS. Additionally, Supplier must maintain the confidentiality of the Personal Data being processed. For the avoidance of doubt, Supplier is prohibited from: (i) selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating orally, or in writing, or by electronic or other means Personal Data to another entity (whether affiliated or not); (ii) Processing the Personal Data for Supplier's own cross-contextual behavioral advertising; (iii) retaining, using, or disclosing the Personal Data outside of the relationship between CHS and Supplier; and (iv) combining the Personal Data with any other personal data Processed by Supplier outside of its relationship with CHS, except as expressly permitted by the Primary Agreement.

b. It will notify CHS in writing, which includes notice to privacy@chsinc.com, immediately upon making a determination that it has not met, or can no longer meet, its

combinación, bloqueo, supresión o destrucción.

h. **"Incidente de Seguridad"** significa cualquier acceso ilegítimo o no autorizado a cualquiera de los Datos Personales de CHS almacenados en los equipos del Proveedor o en las instalaciones del Proveedor, o acceso a equipos o instalaciones que resulte en cualquier uso, adquisición, Tratamiento, pérdida, destrucción, daño, divulgación, robo, copia, modificación o alteración no autorizados de los Datos Personales de CHS.

2. Obligaciones del Proveedor.
El Proveedor declara y garantiza que:

a. Tratará los Datos Personales en nombre de CHS, sólo con el propósito de cumplir con sus obligaciones en virtud del Contrato Principal o según lo indicado por escrito por CHS, y de acuerdo con todas las Leyes de Privacidad de Datos aplicables, y los términos y condiciones de esta Adenda, y se abstendrá de Tratar Datos Personales para fines distintos a los indicados por CHS. Además, el Proveedor deberá mantener la confidencialidad de los Datos Personales que se tratan. Para evitar dudas, el Proveedor tiene prohibido: (i) vender, alquilar, liberar, divulgar, difundir, poner a disposición, transferir o de cualquier otra manera comunicar oralmente, por escrito o por medios electrónicos u otros medios Datos Personales a otra empresa (ya sea vinculada o no); (ii) Tratar los Datos Personales para la propia publicidad conductual intercontextual del Proveedor; (iii) retener, usar o divulgar los Datos Personales fuera de la relación entre CHS y el Proveedor; y (iv) combinar los Datos Personales con cualquier otro dato personal tratado por el Proveedor fuera de su relación con CHS, excepto según lo expresamente autorizado por el Contrato Principal.

b. Notificará a CHS por escrito, lo que incluye una notificación a privacy@chsinc.com, inmediatamente después de determinar que no ha cumplido o ya no puede cumplir con sus obligaciones en virtud de la Sección 2(a) de esta Adenda. En tal caso, el Proveedor deberá acatar las instrucciones escritas de CHS, incluyendo la instrucción de cesar el Tratamiento de

obligations under Section 2(a) of this Addendum. In such case, Supplier will abide by CHS's written instructions, including instructions to cease further Processing of the Personal Data, and shall take any necessary steps to remediate any Processing of such Personal Data not in accordance with Section 2(a) of this Addendum.

c. It will submit its data processing facilities, data files and documentation needed for Processing the Personal Data to auditing and/or review by CHS or any independent auditor or inspection entity reasonably selected by CHS to ascertain compliance with this Addendum upon the request of CHS, with reasonable notice and during normal business hours. Any such data and documentation disclosed in the course of such audit shall be rendered confidential for the purposes of confidentiality obligation, if any under any Primary Agreement between Supplier and CHS.

d. It will obtain the prior written approval of CHS, which includes email notice to privacy@chsinc.com, to disclose Personal Data to any third party or otherwise allow any third party to access Personal Data; and, in such an event, it shall: (i) enter into a written agreement with the third-party subprocessor that imposes obligations substantially similar to those set forth in this Addendum as required under applicable Data Privacy Laws; (ii) impose the same privacy and security requirements on any such third party to which Supplier is subject under this Addendum; (iii) remain responsible for any such third party's actions with respect to the Personal Data; and (iv) provide to CHS, at least 30 days before disclosing or allowing access to any such Personal Data, a list detailing the name and address of all such third parties to which it discloses or allows access to Personal Data, including the locations of such third party's servers hosting or Processing Personal Data, in order to allow CHS to evaluate whether supplemental data processing agreements or other controls are needed to protect Personal Data and/or

los Datos Personales, y deberá tomar las medidas necesarias para resolver cualquier Tratamiento de dichos Datos Personales que no se ajuste a la Sección 2(a) de esta Adenda.

c. Someterá sus instalaciones de tratamiento de datos, archivos de datos y documentación necesarios para el Tratamiento de los Datos Personales a auditoría y/o revisión por parte de CHS o de cualquier auditor independiente o entidad de inspección que CHS seleccione razonablemente para verificar el cumplimiento de esta Adenda, a solicitud de CHS, con un preaviso razonable y durante el horario laboral habitual. Todos los datos y la documentación revelados durante dicha auditoría se considerarán confidenciales a efectos de la obligación de confidencialidad, si la hubiere, en virtud del Contrato Principal entre el Proveedor y CHS.

d. Obtendrá la aprobación previa por escrito de CHS, que incluye una notificación por correo electrónico a privacy@chsinc.com, para divulgar Datos Personales a cualquier tercero o de otro modo permitir que cualquier tercero acceda a Datos Personales; y, en tal caso, deberá: (i) celebrar un acuerdo escrito con el subencargado externo que imponga obligaciones sustancialmente similares a las establecidas en esta Adenda según lo exijan las Leyes de Privacidad de Datos aplicables; (ii) imponer los mismos requisitos de privacidad y seguridad a dicho tercero a los que está sujeto el Proveedor en virtud de esta Adenda; (iii) seguir siendo responsable de las acciones de dicho tercero con respecto a los Datos Personales; y (iv) proporcionar a CHS, al menos 30 días antes de divulgar o permitir el acceso a dichos Datos Personales, una lista que detalle el nombre y la dirección de todos los terceros a los que divulga o permite el acceso a Datos Personales, incluyendo las ubicaciones de los servidores de dichos terceros que almacenan o tratan Datos Personales, para permitir que CHS evalúe si se necesitan acuerdos complementarios de tratamiento de datos u otros controles para proteger los Datos Personales y/o para decidir si rechaza la aprobación para la subcontratación a dichos terceros. El

to decide whether to decline approval for subcontracting to any such third parties. The Supplier shall also notify CHS in writing of any intended changes concerning the addition or replacement of third-party subprocessors, thereby providing the CHS the opportunity to object to such changes in a timely manner. Supplier will be held liable for any and all actions or inactions by itself or its subcontractor with regard to the violation of this Addendum.

e. It will provide assistance to CHS as may be reasonably necessary for CHS to comply with applicable data protection laws, including, but not limited to, (i) assisting CHS in responding to data subject requests for exercising data subject rights under applicable Data Privacy Laws; (ii) assisting CHS in responding to data protection authority or other regulatory requests for information related to Supplier's Processing; (iii) providing all information necessary related to Supplier's Processing for CHS to demonstrate compliance with applicable data protection laws; and (iv) providing reasonable assistance to CHS where CHS is conducting a privacy or transfer impact assessment. Specifically, Supplier agrees that it has the technical ability to and shall assist CHS with securely deleting Personal Data, as well as providing CHS with a list of Personal Data elements about a specific individual held by Supplier on CHS's behalf, upon CHS's request and within 15 days of receiving such request.

f. Promptly, but within no later than forty-eight (48) hours, notify CHS if it receives a request for subject access, rectification, cancellation, objection, restriction, data portability, or revocation of consent for the Processing of Personal Data, or any other data protection related requests. Supplier shall not respond to such requests directly, unless expressly authorized by the CHS in writing. Should any court, government agency or law enforcement agency contact Supplier with a demand for CHS's

Proveedor también notificará a CHS por escrito sobre cualquier cambio previsto con respecto a la adición o sustitución de subencargados externos, brindando así a CHS la oportunidad de oponerse a dichos cambios de manera oportuna. El Proveedor será responsable de todas y cada una de las acciones u omisiones de sí mismo o de su subcontratista con respecto al incumplimiento de esta Adenda.

e. Brindará asistencia a CHS según sea razonablemente necesario para que CHS cumpla con las leyes de protección de datos aplicables, incluyendo, sin limitación, (i) ayudar a CHS a responder a las solicitudes de los interesados para ejercer los derechos de los interesados bajo las Leyes de Privacidad de Datos aplicables; (ii) ayudar a CHS a responder a las autoridades de protección de datos u otras solicitudes regulatorias para obtener información relacionada con el Procesamiento del Proveedor; (iii) proporcionar toda la información necesaria relacionada con el Procesamiento del Proveedor para que CHS demuestre el cumplimiento con las leyes de protección de datos aplicables; y (iv) brindar asistencia razonable a CHS cuando CHS esté realizando una evaluación de impacto de la privacidad o transferencia. Específicamente, el Proveedor acepta que tiene la capacidad técnica para ayudar y deberá ayudar a CHS a eliminar de forma segura los Datos Personales, así como a proporcionar a CHS una lista de elementos de Datos Personales sobre una persona específica en poder del Proveedor en representación de CHS, a solicitud de CHS y dentro de los 15 días posteriores a la recepción de dicha solicitud.

f. Notificará a CHS de inmediato, en un plazo no mayor a cuarenta y ocho (48) horas, en caso de recibir una solicitud de acceso, rectificación, cancelación, objeción, restricción, portabilidad de datos o revocación del consentimiento para el procesamiento de datos personales, o cualquier otra solicitud relacionada con la protección de datos. El Proveedor no responderá a dichas solicitudes directamente, salvo autorización de CHS expresamente por escrito en contrario. Si algún tribunal, agencia gubernamental o autoridad de aplicación de la ley se

Data, Supplier will direct the law enforcement agency to request such information directly from CHS. As part of this effort, Supplier may provide CHS's basic contact information to the agency. If compelled to disclose CHS's Data to law enforcement, then Supplier will promptly, and without any undue delay, notify CHS and deliver a copy of the request (except where Supplier is legally prohibited from doing so) to allow CHS to seek a protective order or any other appropriate remedy. To the extent permitted by applicable law, Supplier shall take all reasonable actions to prevent disclosure of CHS Personal Data to a government agency and/or in response to a legal demand such as subpoena or similar demand, without CHS's prior express written consent. If and only to the extent that is not legally possible, Supplier will notify CHS in advance of any disclosure and provide CHS with the opportunity to object, unless prohibited by applicable law.

comunicara con el Proveedor para solicitar los Datos de CHS, el Proveedor le deberá indicar a dicha autoridad que deberá solicitar dicha información directamente a CHS. Como parte de este esfuerzo, el Proveedor podrá proporcionar la información de contacto básica de CHS a la autoridad. Si se viera obligado a divulgar los Datos de CHS a dichas autoridades, el Proveedor deberá notificar a CHS de inmediato y sin demora indebida y entregar una copia de la solicitud (salvo que el Proveedor tenga prohibido hacerlo) para que CHS pueda solicitar una orden de protección o cualquier otro recurso apropiado. En la medida permitida por la legislación aplicable, el Proveedor deberá tomar todas las medidas razonables para evitar la divulgación de los Datos Personales de CHS a una agencia gubernamental o en respuesta a una orden judicial, tal como una citación judicial o similar, sin el consentimiento previo y expreso por escrito de CHS. Si y sólo hasta el punto en que no fuera legalmente posible, el Proveedor deberá notificar a CHS con antelación sobre cualquier divulgación y le brindará la oportunidad de oponerse, salvo que la legislación aplicable lo prohíba.

3. **Information Security Program.** With respect to the Personal Data transferred to or received by Supplier under the Primary Agreement(s), Supplier has implemented, and will maintain, a comprehensive written information security program ("Information Security Program") that includes administrative, technical, organizational and physical safeguards to ensure the confidentiality, security, integrity, and availability of Personal Data and to protect against unauthorized access, use, disclosure, alteration or destruction of Personal Data. Supplier shall regularly assess and update the Information Security Program to reflect new risks or changes in applicable laws and regulations but shall not make any changes that would materially alter or reduce the measures set out in Supplier's Information Security Program. *Where Personal Data of Korean data subjects is involved, the Information Security Program shall also include such safeguards as are required by applicable law, including, but*

3. **Programa de Seguridad de la Información.** Con respecto a los Datos Personales transferidos al Proveedor o recibidos por este en virtud del/de los Contrato(s) Principal(es), el Proveedor ha implementado y mantendrá un programa integral de seguridad de la información por escrito (el "Programa de Seguridad de la Información") que incluye medidas de protección administrativas, técnicas, organizativas y físicas para garantizar la confidencialidad, seguridad, integridad y disponibilidad de los Datos Personales, así como para protegerlos contra el acceso, uso, divulgación, alteración o destrucción no autorizados. El Proveedor evaluará y actualizará periódicamente el Programa de Seguridad de la Información para reflejar nuevos riesgos o cambios en las leyes y normativas aplicables, pero no realizará cambios que alteren o reduzcan significativamente las medidas establecidas en dicho Programa. *Cuando se trate de datos personales de titulares de datos coreanos, el Programa de Seguridad de la Información también deberá incluir las medidas de*

not limited to, the Personal Information Protection Act, the Enforcement Decree thereof and the Standards for Measures Ensuring the Safety of Personal Information.

a. *These technical and organizational measures are further outlined in Annex I to this Addendum.*

4. **Security Incident.** Supplier shall notify CHS immediately, and no later than 48 hours after discovery, in writing in the event that: (i) any Personal Data is disclosed or is suspected to have been disclosed by Supplier in violation of the Primary Agreement and/or this Addendum, or applicable Data Privacy Laws or (ii) Supplier discovers, is notified of, or suspects that a Security Incident involving Personal Data has occurred, may have occurred, or may occur.

    a. If the Primary Agreement provides for a specific CHS contact, Supplier will notify that contact and also send an e-mail notification to CHSinformationsecurity@chsinc.com. If the agreement or other terms and conditions under which Supplier provides goods, services, or software to the CHS do not provide for a specific contact, Supplier will notify CHS Information Security by e-mail at CHSinformationsecurity@chsinc.com and/or IT Service Center Phone: 651-355-5555 or 800-852-8185. Supplier will also provide to CHS any other notice required by law.

    b. Supplier shall cooperate fully in the investigation of the Security Incident, indemnify and reimburse CHS for any and all damages, losses, fees, fines or costs (whether direct, indirect, special or consequential), including reasonable attorneys' fees and costs, incurred as a result of such incident, and remedy any harm or potential harm caused by such incident. To the extent that a Security Incident gives rise to a need, in CHS's sole judgment to provide (i) notification to public authorities, individuals, or other persons, or (ii) undertake other remedial measures (including, without limitation, notice,

protección requeridas por la ley aplicable, incluyendo, pero sin limitación, la Ley de Protección de Información Personal, el Decreto de Aplicación de la misma y las Normas para Medidas que Garantizan la Seguridad de la Información Personal.

a. *Estas medidas técnicas y organizativas se describen con más detalle en el Anexo I de la presente Adenda.*

4. **Incidente de Seguridad.** El Proveedor deberá notificar a CHS inmediatamente, y en un plazo no mayor a 48 horas después del hallazgo, por escrito en el caso de que: (i) cualquier Dato Personal sea divulgado o se sospeche que haya sido divulgado por el Proveedor en incumplimiento del Contrato Principal y/o esta Adenda, o las Leyes de Privacidad de Datos aplicables o (ii) el Proveedor descubra, sea notificado o sospeche que ha ocurrido, que puede haber ocurrido o que puede ocurrir un Incidente de Seguridad que involucra Datos Personales.

    a. Si el Contrato Principal estipula un contacto específico de CHS, el Proveedor deberá notificar a dicho contacto y también enviará una notificación por correo electrónico a CHSinformationsecurity@chsinc.com. Si el contrato u otros términos y condiciones en virtud de los cuales el Proveedor proporciona bienes, servicios o software a CHS no estipulan un contacto específico, el Proveedor deberá notificar al sector de Seguridad de la Información de CHS por correo electrónico a CHSinformationsecurity@chsinc.com o al Centro de Servicios de IT a los teléfonos: 651-355-5555 o 800-852-8185. El Proveedor también deberá enviar a CHS cualquier otra notificación requerida por ley.

    b. El Proveedor deberá cooperar plenamente en la investigación del Incidente de Seguridad, indemnizar y reembolsar a CHS por todos los daños y perjuicios, pérdidas, honorarios, multas o gastos (ya sean directos, indirectos, especiales o resultantes), incluyendo honorarios y gastos razonables de abogados, incurridos como resultado de dicho incidente, y solucionar cualquier daño o daño potencial causado por dicho incidente. En la medida en que un Incidente de Seguridad dé lugar a una necesidad, a criterio exclusivo de CHS, deberá proporcionar (i) notificación

credit monitoring services and the establishment of a call center to respond to inquiries (each of the foregoing a "Remedial Action(s)")), at CHS's request, Supplier shall, at Supplier's cost, undertake such Remedial Actions. The timing, content and manner of effectuating any notices shall be determined by CHS in its sole discretion.

c. Except as is required by law or as otherwise required to act exigently to mitigate or avoid further harm or damage to persons or property, Supplier will not inform any third party of any Security Incident without first obtaining CHS's prior written consent. Where Supplier informs any third party of a Security Incident as required by law or as otherwise required to act exigently to mitigate or avoid further harm or damage to persons or property, Supplier will give notice to the CHS concurrently with such other notice.

d. To the extent reasonably requested by the CHS, following notification of a Security Incident, Supplier's cooperation regarding the investigation of the Security Incident shall include: (i) providing CHS with physical access to the facilities and operations affected; (ii) facilitating interviews with Supplier's employees and others involved in the matter; and (iii) making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably required by the CHS or its designees. Supplier shall also take proactive measures to mitigate the risk of further damage from the Security Incident, including implementing any measures required by law or as directed by CHS.

5. Cross-Border Transfer of Personal Data. Supplier shall not Process Personal Data in a

a autoridades públicas, individuos u otras personas, o (ii) tomar otras medidas correctivas (incluyendo, sin limitación, aviso, servicios de monitoreo de crédito y el establecimiento de un centro de llamadas para responder consultas (cada uno de los anteriores, en adelante, "Acción(es) Correctiva(s)")), a solicitud de CHS, el Proveedor deberá, a expensas del Proveedor, iniciar dichas Acciones Correctivas. El momento, el contenido y la forma de efectuar cualquier notificación serán determinados por CHS a su entera discreción.

c. Salvo que lo exija la ley o que se requiera actuar con urgencia para mitigar o evitar daños o perjuicios adicionales a personas o bienes, el Proveedor no deberá informar a terceros sobre ningún Incidente de Seguridad sin obtener previamente el consentimiento por escrito de CHS. Si el Proveedor informa a un tercero sobre un Incidente de Seguridad, según lo exija la ley o que se requiera actuar con urgencia para mitigar o evitar daños o perjuicios adicionales a personas o bienes, deberá notificar a CHS simultáneamente con dicha notificación.

d. En la medida en que CHS lo solicite razonablemente, con posterioridad a la notificación de un Incidente de Seguridad, la cooperación del Proveedor en la investigación del Incidente de Seguridad deberá incluir: (i) proporcionar a CHS acceso físico a las instalaciones y operaciones afectadas; (ii) facilitar entrevistas con los empleados del Proveedor y otras personas involucradas en la cuestión; y (iii) poner a disposición todos los registros, archivos, informes de datos y demás materiales pertinentes necesarios para cumplir con la legislación, las reglamentaciones y los estándares de la industria aplicables, o según lo requiera razonablemente CHS o sus designados. El Proveedor también deberá adoptar medidas proactivas para mitigar el riesgo de daños adicionales derivados del Incidente de Seguridad, incluyendo la implementación de cualquier medida exigida por la ley o según lo indique CHS.

5. Transferencia de Datos fuera del país. El Proveedor no deberá tratar Datos Personales en una

jurisdiction outside of the agreed Processing location without the written consent of CHS. To the extent that Personal Data includes information about individuals who are located in the European Economic Area (“EEA”), the UK, Argentina or Switzerland, and Supplier or any subcontractors store or otherwise obtain access to such Personal Data outside of the EEA, UK, Argentina or Switzerland, the Supplier agrees to Process this Personal Data in accordance with the EU Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to the Commission Implementing Decision (EU) 2021/914, Module Two, which is incorporated by reference herein (“Model Processor Contract” or “SCC”), the UK International Data Transfer Addendum ("UK Addendum"), which are incorporated here by reference, for Personal Data on which the UK data protection laws apply, and for Personal Data on which the Swiss or Argentine data protection laws apply including the specific Swiss or Argentine local law amendments to the Model Processor Contract. To the extent that Personal Data includes information about individuals who are located in Brazil, and were located in Brazil at the moment that the information was collected and Supplier or any subcontractors store or otherwise obtain access to such Personal Data outside of Brazil, the Supplier agrees to Process this Personal Data in accordance with the Brazilian Model Clauses ("BMC"), as published by the Brazilian Data Protection Authority (“ANPD”), which are incorporated here as Annex II. To the extent that Supplier Processes Personal Data in a particular jurisdiction other than the EEA, UK, Argentina or Switzerland, and such Processing would be prohibited by applicable privacy laws in the absence of the implementation of terms comparable to the Model Processor Contract, Supplier shall Process all such Personal Data in accordance with the Model Processor Contract, and for such purposes, references to EU/EEA jurisdictions shall be deemed to be references to the relevant non-EU/EEA jurisdictions as applicable.

a. With respect to the Model Processor Contract: (i) the signature to this Addendum constitutes signature to the Model Processor Contract,

jurisdicción fuera de la locación de tratamiento acordada sin el consentimiento por escrito de CHS. En la medida en que los Datos Personales incluyan información sobre personas que se encuentran en el Espacio Económico Europeo ("EEE"), el Reino Unido, Argentina o Suiza, y el Proveedor o cualquier subcontratista almacene o acceda de otro modo a dichos Datos Personales fuera del EEE, el Reino Unido, Argentina o Suiza, el Proveedor se compromete a procesar estos Datos Personales de conformidad con las Cláusulas Contractuales Tipo de la UE para la Transferencia de Datos Personales a Terceros Países, de conformidad con la Decisión de Ejecución (UE) 2021/914 de la Comisión, Módulo Dos, que se incorpora por referencia al presente documento ("Contrato Modelo de Tratamiento" o "SCC"), el Anexo de Transferencia Internacional de Datos del Reino Unido ("Anexo del Reino Unido"), que se incorporan al presente para fines de referencia, para los Datos Personales a los que se aplican las leyes de protección de datos del Reino Unido, y para los Datos Personales a los que se aplican las leyes de protección de datos suizas o argentinas, incluidas las modificaciones específicas de la legislación local suiza o argentina al Contrato Modelo de Encargado del Tratamiento. En la medida en que los Datos Personales incluyan información sobre personas que se encuentran en Brasil y que se encontraban en Brasil en el momento en que se recopiló la información, y el Proveedor o cualquier subcontratista almacene u obtenga acceso a dichos Datos Personales fuera de Brasil, el Proveedor acepta procesar estos Datos Personales de conformidad con las Cláusulas Modelo Brasileñas ("BMC"), publicadas por la Autoridad Brasileña de Protección de Datos ("ANPD"), que se incorporan al presente como Anexo II. En la medida en que el Proveedor trata Datos Personales en una jurisdicción particular distinta del EEE, el Reino Unido, Argentina o Suiza, y dicho Tratamiento estuviera prohibido por las leyes de privacidad aplicables en ausencia de la implementación de términos comparables a los del Contrato Modelo de Encargado de Tratamiento, el Proveedor deberá tratar todos esos Datos Personales de conformidad con el Contrato Modelo de Encargado de Tratamiento y, para tales fines, las referencias a jurisdicciones de la UE/EEE se considerarán referencias a las jurisdicciones pertinentes no pertenecientes a la UE/EEE, según corresponda.

a. Con respecto al Contrato Modelo de Encargado de tratamiento: (i) la firma de esta Adenda constituye la firma del Contrato Modelo de Encargado de

including the appendices thereto; (ii) each of CHS and/or CHS's subsidiaries established in the EEA, UK, Argentina or Switzerland shall be deemed for the purposes of this Addendum to be the "data exporter"; (iii) Supplier and each subcontractor that stores, accesses, or otherwise Processes such Personal Data shall be deemed for the purposes of this Addendum to be a "data importer"; (iv) the data Processing activities in Appendix I to the Model Processor Contract shall be as described in Appendix 1 to this Addendum; and (v) the data security measures in Appendix II to the Model Processor Contract shall be those identified in Annex I to this Addendum; and the Primary Agreement(s). For the purposes of the UK Addendum: (a) Table 1 shall be completed with the information regarding the parties set out in Appendix 1; (b) Table 2 shall be completed with the information in this Section; (c) Table 3 shall be completed by referring to the corresponding information in Appendix 1 and Annex I to this Addendum; and (d) Table 4 the option of "Exporter" shall be selected.

b. With respect to the Model Processor Contract, the following is acknowledged and agreed to by both the CHS and Supplier: (i) Clause 7 Docking Clause shall apply; (ii) the data exporter is to receive 60 days' notice pursuant to Clause 9(a); (iii) Supplier must obtain specific authorization (as detailed above in Section 2(d) for the appointment of subprocessors; (iv) the optional language under Clause 11(a) (Optional Redress with Independent Resolution Body) shall not apply; the parties choose the supervisory authority of Spain'sAgencia Española de Protección de Datos (AEPD); the governing law with respect to Clause 17, Option 1 (Governing Law) shall apply and the "Member State" shall be Spain, Model Processor Contract shall be governed by the laws of the jurisdiction applicable CHS exporter; and (x) for purposes of Clause 18

tratamiento, incluyendo sus documentos adjuntos; (ii) cada una de las sedes de CHS y/ de las subsidiarias de CHS establecidas en el EEE, el Reino Unido, Argentina o Suiza se considerará, a los efectos de esta Adenda, el «exportador de datos»; (iii) el Proveedor y cada subcontratista que almacene, acceda a o de cualquier otro modo trate dichos Datos Personales se considerará, a los efectos de esta Adenda, un «importador de datos»; (iv) las actividades de Tratamiento de datos del Anexo I del Contrato Modelo de Encargado de Tratamiento serán las descritas en el Anexo 1 de esta Adenda; y (v) las medidas de seguridad de los datos del Anexo II del Contrato Modelo de Encargado de tratamiento serán las identificadas en el Anexo I de esta Adenda; y el(los) Acuerdo(s) Principal(es). A los efectos del Anexo del Reino Unido: (a) El Cuadro 1 se deberá completar con la información relativa a las partes que se establece en el Anexo 1; (b) el Cuadro 2 se deberá completar con la información de este Artículo; (c) el Cuadro 3 se deberá completar haciendo referencia a la información correspondiente del Anexo 1 y del Anexo I de esta Adenda; y (d) en el Cuadro 4 se seleccionará la opción "Exportador".

b. Con respecto al Contrato Modelo de Encargado de tratamiento, tanto CHS como el Proveedor reconocen y acuerdan lo siguiente: (i) se aplicará la Cláusula de Incorporación de la Cláusula 7; (ii) el exportador de datos deberá recibir un aviso de 60 días de conformidad con la Cláusula 9(a); (iii) el Proveedor deberá obtener una autorización específica (tal como se detalla anteriormente en la Sección 2(d) para el nombramiento de subencargados); (iv) el lenguaje opcional de la Cláusula 11(a) (Reparación Opcional con Organismo de Resolución Independiente) no se aplicará; las partes eligen la autoridad de control de la Agencia Española de Protección de Datos (AEPD); la ley aplicable con respecto a la Cláusula 17, Opción 1 (Ley Aplicable) se aplicará y el "Estado Miembro" será España, el Contrato Modelo de Encargado de tratamiento se regirá por las leyes de la jurisdicción aplicable al exportador de CHS; y (x) a los efectos de la Cláusula 18 (Elección de Foro

(Choice of Forum and Jurisdiction), any disputes arising from the Model Processor Contract shall be resolved by the courts of Spain.

c. The Swiss local law amendments to the Model Processor Contract are the following: 1. Supervisory Authority: The Federal Data Protection and Information Commissioner is the competent supervisory authority; 2. Applicable Law for Contractual Claims under Clause 17: Swiss law (or the law of a country that allows and grants rights as a third party beneficiary for contractual claims regarding data transfers pursuant to the Federal Act on Data Protection "FADP"); 3. Member State / European Union: Switzerland is to be considered as a Member State within the meaning of the Model Processor Contract so that data subjects among others are entitled to file claims according to clause 18c of the Model Processor Contract at their habitual residence in Switzerland; 4. References to the General Data Protection Regulation and the Regulation (EU) 2016/679 are to be understood as references to the FADP; 5. Personal Data: Until the revised FADP enters into force on September 1, 2023 that does no longer protect data of legal persons but only data of natural persons, the Model Processor Contract also applies to data of legal persons.

d. With respect to Personal Data of Korean data subjects: Supplier acknowledges that cross-border transfers of such data require notification to the data subject of: (i) the Personal Data to be transferred; (ii) the country, time and method of transfer; (iii) the name and contact information of the recipient; (iv) the purpose of use and the period of retention by the recipient; and (v) the method and procedure for objecting to the transfer and the consequences of such objection. The data subject's consent to such transfers shall also be obtained where required by applicable law, such as where the transfer is not necessary for CHS to perform its underlying contract with the data

y Jurisdicción), cualquier disputa que surja del Contrato Modelo de Encargado de tratamiento se deberá resolver en los tribunales de España.

c. Las modificaciones de la legislación local suiza al Contrato Modelo de Encargado de tratamiento son las siguientes: 1. Autoridad de control: El Comisionado Federal de Protección de Datos e Información es la autoridad de control competente; 2. Ley aplicable a los reclamos contractuales según la Cláusula 17: Ley suiza (o la ley de un país que permita y otorgue derechos como tercero beneficiario para reclamos contractuales relacionados con las transferencias de datos de conformidad con la Ley Federal de Protección de Datos "FADP"); 3. Estado miembro / Unión Europea: Suiza debe considerarse un Estado miembro en el sentido del Contrato Modelo de Encargado de tratamiento, de modo que los interesados, entre otros, tienen derecho a presentar reclamos de acuerdo con la cláusula 18c del Contrato Modelo de Encargado de tratamiento en su residencia habitual en Suiza; 4. Las referencias al Reglamento General de Protección de Datos y al Reglamento (UE) 2016/679 deben entenderse como referencias a la FADP; 5. Datos personales: Hasta que entre en vigor el FADP revisado el 1 de septiembre de 2023, que ya no protege los datos de personas jurídicas sino únicamente los datos de personas físicas, el Contrato Modelo de Encargado de tratamiento también se aplica a los datos de personas jurídicas.

d. Con respecto a los Datos Personales de titulares de datos coreanos: El Proveedor reconoce que las transferencias fuera del país de dichos datos requieren la notificación al titular de los datos de: (i) los Datos Personales a transferir; (ii) el país, la fecha y el método de la transferencia; (iii) el nombre y la información de contacto del destinatario; (iv) la finalidad del uso y el período de conservación por parte del destinatario; y (v) el método y el procedimiento para oponerse a la transferencia y las consecuencias de dicha objeción. También se deberá obtener el consentimiento del titular de los datos para dichas transferencias cuando lo exija la legislación aplicable, por ejemplo, cuando la transferencia no sea necesaria para que

subject. Supplier shall assist CHS in complying with these obligations.

e. With respect to Personal Data of Brazilian data subjects: (i) the BMC shall be executed as provided in Annex II; (ii) each of CHS and/or CHS's subsidiaries established in the Brazil shall be deemed for the purposes of this Addendum to be the "data exporter"; (iii) Supplier and each subcontractor that stores, accesses, or otherwise Processes such Personal Data shall be deemed for the purposes of this Addendum to be a "data importer"; (v) the ANPD is the competent supervisory authority under the BMC; and (vi) in the event that any provision of this Annex contradicts, directly or indirectly, the BMC, the BMC shall prevail.

f. With respect to Personal Data of Argentine data subjects: the Argentine local law amendments to the Model Processor Contract are the following: 1. "Data Privacy Law" shall mean Personal Data Protection Law No. 25,326 and Regulatory Decree No. 1558/2001, as amended, complemented and/or replaced in the future; "Personal Data", "Sensitive Personal Data", "Processing", "Controller" and "Data Subject" shall have the meaning set forth under the Data Privacy Law; "authority" or "supervisory authority" shall mean the National Directorate of Personal Data Protection of Argentina; "data exporter" shall mean the party responsible for Processing who transfers the Personal Data; "data importer" or "Processor" shall mean the service provider as set forth under Section 25 of Data Privacy Law, that is established outside Argentina and agrees to receive from data exporter Personal Data for further Processing in accordance with the terms of the Primary Agreement and this Addendum; 2. Data Subjects may require data importer, as third-party beneficiaries, to comply with the provisions of Data Privacy Law; 3. Data importer accepts that the supervisory authority exercises its powers within the limits granted by

CHS cumpla con su contrato subyacente con el titular de los datos. El Proveedor deberá asistir a CHS en el cumplimiento de estas obligaciones.

e. Con respecto a los Datos Personales de titulares de datos brasileños: (i) el BMC se ejecutará según lo dispuesto en el Anexo II; (ii) cada una de las sedes de CHS y/o subsidiarias de CHS establecidas en Brasil se considerará, a los efectos de esta Adenda, como el "exportador de datos"; (iii) el Proveedor y cada subcontratista que almacene, acceda o de otro modo procese dichos Datos Personales se considerará, a los efectos de esta Adenda, como un "importador de datos"; (v) la ANPD es la autoridad de supervisión competente en virtud del BMC; y (vi) en caso de que alguna disposición de este Anexo contradiga, directa o indirectamente al BMC, el BMC prevalecerá.

f. Con respecto a los Datos Personales de titulares de datos argentinos: las modificaciones de la ley local argentina al Contrato Modelo de Encargado de tratamiento son las siguientes: 1. "Ley de Privacidad de Datos" significará la Ley de Protección de Datos Personales N.º 25.326 y el Decreto Reglamentario N.º 1558/2001, según sus modificaciones, complementos y/o reemplazos en el futuro; "Datos Personales", "Datos Personales Sensibles", "Tratamiento", "Responsable" y "Titular de Datos" tendrán el significado establecido en la Ley de Privacidad de Datos; "autoridad" o "autoridad supervisora" significará la Dirección Nacional de Protección de Datos Personales de Argentina; "exportador de datos" significará la parte responsable del Procesamiento que transfiere los Datos Personales; "importador de datos" o "Encargado de tratamiento" significará el proveedor de servicios según lo establecido en el Articulo 25 de la Ley de Privacidad de Datos, que está establecido fuera de Argentina y acepta recibir del exportador de datos los Datos Personales para su posterior Tratamiento de conformidad con los términos del Contrato Principal y esta Adenda; 2. Los Titulares de los Datos pueden requerir al importador de datos, como terceros beneficiarios, que cumpla con las disposiciones de la Ley de Privacidad de Datos; 3. El importador de

Data Privacy Law, accepting its powers of control and sanction, granting the supervisory authority for such purposes, in what is pertinent, the capacity of third-party beneficiary; 4. Data exporter warrants and undertakes that (i) it has informed Data Subjects that their Personal Data could be transferred to a third country that does not offer an adequate level of data protection, (ii) if Data Subjects or the supervisory authority -as a third party-beneficiaries- exercise their rights or powers, as the case may be, data exporter will respond the request within the terms set forth by Data Privacy Law, and (iii) it shall keep a list of sub-Processing contracts entered into by the data importer, which shall be updated at least once a year, and that the list shall be available for the supervisory authority; 5. Data importer warrants and undertakes that: (a) it has verified that its local legislation does not prevent data importer from fulfilling the obligations, representations and principles included in the Primary Agreement and the Addendum, and it shall promptly notify data exporter about the existence of any disposition of such nature as soon as it becomes aware; (b) it will promptly notify the data exporter about: (i) any legally binding request for disclosure of the Personal Data issued by a law enforcement authority, unless otherwise prohibited by applicable regulations; (ii) every accidental or unauthorized access to Personal Data; and (iii) every request received directly from Data Subjects; (c) it will not assign or transfer Personal Data to third parties except that the assignment or transfer is required by law or a competent authority, in which case it will verify that the requesting authority offers adequate guarantees of compliance with the principles the Data Privacy Law, and the rights of the Data Subjects; (d) it will process the requests and consultations received from Data Subjects (or from data exporter acting on Data Subject's behalf) and the supervisory authority, who shall be considered to act as third-party

datos acepta que la autoridad supervisora ejerza sus facultades dentro de los límites otorgados por la Ley de Privacidad de Datos, y aceptará sus facultades de control y sanción, y otorgará a la autoridad supervisora para tales fines, en lo que sea pertinente, la calidad de tercero beneficiario; 4. El exportador de datos garantiza y se compromete a que (i) ha informado a los titulares de los datos que sus datos personales podrían ser transferidos a un tercer país que no ofrece un nivel adecuado de protección de datos, (ii) si los titulares de los datos o la autoridad supervisora, en carácter de terceros beneficiarios, ejercen sus derechos o facultades, según sea el caso, el exportador de datos responderá la solicitud dentro de los términos establecidos por la Ley de Privacidad de Datos, y (iii) mantendrá una lista de los contratos de subtratamiento celebrados por el importador de datos, que se actualizará al menos una vez al año, y que la lista estará a disposición de la autoridad supervisora; 5. El importador de datos garantiza y se compromete a que: (a) ha verificado que su legislación local no impide que el importador de datos cumpla con las obligaciones, declaraciones y principios incluidos en el Contrato Principal y la Adenda, y notificará de inmediato al exportador de datos sobre la existencia de cualquier disposición de dicha naturaleza tan pronto como tenga conocimiento; (b) notificará de inmediato al exportador de datos sobre: (i) cualquier solicitud legalmente vinculante para la divulgación de los Datos Personales emitida por una autoridad de aplicación de la ley, salvo que esté prohibido por las reglamentaciones aplicables; (ii) todo acceso accidental o no autorizado a los Datos Personales; y (iii) toda solicitud recibida directamente de los Titulares de los Datos; (c) no cederá ni transferirá Datos Personales a terceros, salvo que la cesión o transferencia sea requerida por ley o una autoridad competente, en cuyo caso verificará que la autoridad solicitante ofrezca garantías adecuadas de cumplimiento de los principios de la Ley de Privacidad de Datos y los derechos de los Titulares de los Datos; (d) procesará las solicitudes y consultas recibidas de los Titulares de los Datos (o

beneficiaries; and (e) in case of sub-Processing of Personal Data, it will have had previously informed the data exporter and obtained its prior consent in writing; 6. Data exporter and data importer agree that as regards the Processing of Personal Data the Primary Agreement and the Addendum will be governed by the laws of Argentina, and that in case of conflict related to the protection of Personal Data the judicial and administrative jurisdiction of Argentina will be competent; 7. Data exporter and data importer agree that, upon termination of the provision of Processing services, data importer and the sub-processor, if any, shall, at the choice of the data exporter, return all the Personal Data transferred and the copies thereof to the data exporter or destroy all the Personal Data and certify the same.

del exportador de datos que actúe en nombre del Titular de los Datos) y la autoridad de control, quienes serán considerados terceros beneficiarios; y (e) en caso de subtratamiento de Datos Personales, deberá haber informado previamente al exportador de datos y obtenido su consentimiento previo por escrito; 6. El exportador de datos y el importador de datos acuerdan que, en lo que respecta al Tratamiento de Datos Personales, el Contrato Principal y la Adenda se regirán por las leyes de Argentina, y que en caso de conflicto relacionado con la protección de Datos Personales será competente la jurisdicción judicial y administrativa de Argentina; 7. El exportador de datos y el importador de datos acuerdan que, al finalizar la prestación de los servicios de Tratamiento, el importador de datos y el subencargado, si lo hubiera, devolverán, a elección del exportador de datos, todos los Datos Personales transferidos y las copias de los mismos al exportador de datos o destruirán todos los Datos Personales y certificarán dicha acción.

6. Miscellaneous Obligations.

a. Supplier shall, upon the CHS's request, promptly execute supplemental data processing agreement(s) with CHS or any of its subsidiaries, provide necessary assistance or take other appropriate steps, to its best efforts, to address cross-border transfer and other requirements if CHS concludes, in its sole judgment, that such supplemental data processing agreement(s), assistances, and steps are necessary to address applicable Data Privacy Laws concerning Personal Data.

b. Supplier will appoint a data protection officer where such appointment is required by data protection laws. The appointed person may be reached by email via the email address provided by Supplier on the signature page of this DPA. Supplier will promptly notify CHS of any change in the data protection officer contact information.

c. Supplier certifies that it understands and will comply, and cause all Supplier personnel to certify that they

6. Obligaciones varias.

a. El Proveedor deberá, a solicitud de CHS, formalizar de inmediato contrato(s) de tratamiento de datos complementarios con CHS o cualquiera de sus subsidiarias, brindar la asistencia necesaria o tomar otras medidas apropiadas, en la medida de sus esfuerzos posibles, para abordar la transferencia fuera del país y otros requisitos si CHS concluye, a su exclusivo criterio, que dicho(s) acuerdo(s) de tratamiento de datos complementarios, asistencia y medidas son necesarios para abordar las Leyes de Privacidad de Datos aplicables con respecto a los Datos Personales.

b. El Proveedor deberá designar un responsable de protección de datos cuando así lo exija la legislación vigente. Se deberá poder contactar a la persona designada por correo electrónico a la dirección proporcionada por el Proveedor en la página de firma de este Contrato de Tratamiento de Datos (CPD). El Proveedor deberá notificar inmediatamente a CHS sobre cualquier cambio en la información

understand and will comply with the requirements of this Addendum.

d. The parties agree that, to the extent such right is clearly established in the Primary Agreement, Supplier may use CHS's Personal Data on the CHS's behalf. In such cases, CHS instructs Supplier to use only de-identified or aggregate information, and, for the sake of clarity, CHS instructs Supplier to first anonymize, aggregate, and/or de-identify the Personal Data as necessary for that purpose. With respect to such de-identified or aggregated information: (1) Supplier shall comply with all applicable laws, including the implementation of: (a) technical safeguards that prohibit reidentification; (b) business processes that specifically prohibit reidentification; (c) business processes to prevent inadvertent release of deidentified information; and (2) Supplier shall make no attempt to reidentify the information.

e. At all times at which Supplier holds CHS's Personal Data, Supplier will have in place a bona fide business continuity plan that will ensure that Supplier is able to continue to provide services when the provision of such services is interrupted for any reason outside of Supplier's reasonable control ("Business Continuity Plan"). Supplier shall maintain and update the Business Continuity Plan at least annually for each of its operational sites related to the provision of services. Supplier will put the Business Continuity Plan in effect if a site becomes unable to perform such services or deliver services for a period of more than five (5) calendar days. Supplier will perform a timely assessment after the occurrence of any event that may delay the performance of maintenance and support or the delivery of services for a period of more than five (5) calendar days. Supplier will activate the Business Continuity Plan if Supplier determines that Supplier will be unable to perform services for a period of more than five (5) calendar days.

de contacto del responsable de protección de datos.

c. El Proveedor certifica que comprende y que cumplirá con los requisitos de esta Adenda, y se asegurará de que todo el personal del Proveedor certifique que comprende y cumpla con los mismos.

d. Las partes acuerdan que, en la medida en que dicho derecho se establezca claramente en el Contrato Principal, el Proveedor podrá utilizar los Datos Personales de CHS en nombre de CHS. En tales casos, CHS instruye al Proveedor a utilizar únicamente información anónima o agregada y, para mayor claridad, CHS instruye al Proveedor a anonimizar, agregar o quitar referencias de identificación personal previamente de los Datos Personales según sea necesario para tal fin. Con respecto a dicha información anónima o agregada: (1) El Proveedor deberá cumplir con todas las leyes aplicables, incluyendo la implementación de: (a) garantías técnicas que prohíban la recuperación de las referencias de identificación personal; (b) procesos comerciales que prohíban específicamente dicha recuperación; (c) procesos comerciales para prevenir la divulgación inadvertida de información anónima; y (2) El Proveedor no intentará recuperar las referencias personales de la información.

e. En todo momento en que el Proveedor tenga en su poder los Datos Personales de CHS, el Proveedor deberá contar con un plan de continuidad empresarial de buena fe que garantice que el Proveedor pueda continuar prestando servicios cuando la prestación de dichos servicios se interrumpa por cualquier motivo fuera del control razonable del Proveedor ("Plan de Continuidad Empresarial"). El Proveedor deberá mantener y actualizar el Plan de Continuidad Empresarial al menos una vez al año para cada uno de sus sitios operativos relacionados con la prestación de servicios. El Proveedor deberá poner en vigor el Plan de Continuidad Empresarial cuando un sitio no pueda realizar dichos servicios o prestar servicios durante un período mayor a cinco (5) días corridos. El Proveedor deberá realizar oportunamente una evaluación después de la ocurrencia de cualquier incidente que pueda retrasar la realización del mantenimiento y el soporte

o la prestación de los servicios durante un período mayor a cinco (5) días corridos. El Proveedor deberá activar el Plan de Continuidad Empresarial si determina que no estará en condiciones de prestar los servicios durante un período mayor a cinco (5) días corridos.

7. **Governing Law.** This Addendum will be governed by and construed in accordance with the laws of the state which govern the Primary Agreement, without regard for its choice of law rules.

7. **Ley que rige.** Esta Adenda se deberá regir e interpretar de conformidad con las leyes del estado que rigen el Contrato Principal, independientemente de sus disposiciones de elección de ley.

8. **Term, Termination, and Effective Date.**

   a. This Addendum shall be effective as of the date last executed by a party (the "Effective Date") and shall remain in full force and effect for so long as the Primary Agreement(s) remains in effect, unless earlier terminated pursuant to Section 8(b).

   b. CHS may terminate this Addendum and/or the Primary Agreement immediately, without judicial notice or resolution and without prejudice to any other remedies, in the event that (i) compliance with the terms of this Addendum by the Supplier would put Supplier in breach of its legal obligations; (ii) the Supplier is in substantial breach of any representations or warranties given by it under this Addendum and fails to cure such breach with (30) days' notice from CHS; (iii) Supplier provides notice to CHS pursuant to Section 2(b) of this Addendum; (iv) a data protection or other regulatory authority or other tribunal or court in the countries in which CHS or its subsidiaries operates finds that there has been a breach of any relevant laws in that jurisdiction by virtue of the Supplier's or CHS's Processing of the Personal Data; or (v) if either party makes an assignment for the benefit of creditors, becomes subject to a bankruptcy proceeding, is subject to the appointment of a receiver, or admits in writing its inability to pay its debts as they become due.

8. **Plazo, Extinción y Fecha de Entrada en Vigencia.**

   a. Esta Adenda entrará en vigencia a partir de la última fecha firmada por una de las partes (la "Fecha de Entrada en Vigencia") y permanecerá en pleno vigor y efecto mientras el o los Contrato(s) Principal(es) permanezca(n) en vigencia, salvo que se extinga antes de ese plazo de conformidad con el Artículo 8(b).

   b. CHS podrá rescindir esta Adenda y/o el Contrato Principal inmediatamente, sin necesidad de notificación o resolución judicial y sin perjuicio de cualquier otro recurso, en caso de que (i) el cumplimiento de los términos de este Adenda por parte del Proveedor lo ponga en incumplimiento de sus obligaciones legales; (ii) el Proveedor incumpla sustancialmente cualquier declaración o garantía otorgada por él en virtud de esta Adenda y no subsane dicho incumplimiento con un aviso de (30) días desde CHS; (iii) el Proveedor notifique a CHS de conformidad con la Sección 2(b) de esta Adenda; (iv) una autoridad de protección de datos u otra autoridad reguladora u otro tribunal o corte en los países en los que opera CHS o sus subsidiarias determine que se ha incumplido alguna ley pertinente en esa jurisdicción en virtud del Procesamiento de los Datos Personales por parte del Proveedor o CHS; o (v) si cualquiera de las partes realiza una cesión en beneficio de los acreedores, se vuelve objeto de un procedimiento de quiebra, está sujeta al nombramiento de un síndico o admite por escrito su incapacidad para pagar sus deudas a su vencimiento.

c. This Addendum shall immediately terminate if all applicable Primary Agreement are terminated for any reason.

d. Upon termination of this Addendum for any reason, the Supplier shall return all Personal Data and all copies of the Personal Data subject to this Addendum to CHS or, at CHS's request, shall destroy (i.e., render the information permanently unreadable and not-reconstructable into a usable format in accordance with the then-current U.S. Department of Defense, or CESG standards, or equivalent data destruction standards, as applicable) all such Personal Data and shall certify to CHS that it has done so.

Signature page to follow

c. Esta Adenda se extinguirá inmediatamente si todos los Contratos Principales aplicables se extinguen por cualquier motivo.

d. Ante la extinción de esta Adenda por cualquier motivo, el Proveedor deberá devolver todos los Datos Personales y todas las copias de los Datos Personales sujetos a esta Adenda a CHS o, a solicitud de CHS deberá destruir (es decir, hacer que la información sea permanentemente ilegible y no reconstruible en un formato utilizable de acuerdo con las normas vigentes en ese momento del Departamento de Defensa de los EE. UU. o CESG, o normas de destrucción de datos equivalentes, según corresponda) todos esos Datos Personales y deberá certificar a CHS que lo ha hecho.

Sigue página de firmas

IN WITNESS WHEREOF, the parties have executed this Addendum and represent that their respective signatories whose signatures appear below are authorized by all necessary corporate action to execute this Addendum.

This Addendum may be executed in one or more counterparts, each of which will be deemed an original, but all of which taken together will constitute one and the same agreement.

Signed by:
[Insert CHS Entity]

_____
Signature

_____
Name

_____
Date

_____
Title

EN PRUEBA DE CONFORMIDAD, las partes han formalizado esta Adenda y declaran que sus respectivos firmantes, cuyas firmas figuran a continuación, están autorizados por todas las acciones corporativas necesarias para formalizar esta Adenda.

Esta Adenda podrá ser formalizada en uno o más ejemplares, cada uno de los cuales se considerará un original, pero todos ellos tomados en conjunto constituirán un único y mismo acuerdo.

Firmado por:
[Insertar sociedad de CHS]

_____
Firma

_____
Nombre

_____
Fecha

_____
Cargo

Supplier

IN WITNESS WHEREOF, the parties have executed this Addendum and represent that their respective signatories whose signatures appear below are authorized by all necessary corporate action to execute this Addendum.

This Addendum may be executed in one or more counterparts, each of which will be deemed an original, but all of which taken together will constitute one and the same agreement.

Signed by:
[Insert Supplier name]

_____
Signature

_____
Name

_____
Date

_____
Title

Email Address of DPO, if applicable

Proveedor

EN PRUEBA DE CONFORMIDAD, las partes han formalizado esta Adenda y declaran que sus respectivos firmantes, cuyas firmas figuran a continuación, están autorizados por todas las acciones corporativas necesarias para formalizar esta Adenda.

Esta Adenda podrá ser formalizada en uno o más ejemplares, cada uno de los cuales se considerará un original, pero todos ellos tomados en conjunto constituirán un único y mismo acuerdo.

Firmado por:
[Insertar el nombre del Proveedor]

_____
Firma

_____
Nombre

_____
Fecha

_____
Cargo

Dirección de correo electrónico del DPO (Responsable de Protección de Datos), si corresponde

APPENDIX 1 TO THE EU STANDARD CONTRACTUAL CLAUSES

This Appendix 1 includes certain details of the Processing of CHS (CHS Inc.) Personal Data as required by Article 28(3) of the GDPR (or as applicable, equivalent provisions of any other data protection law).

Part A. List of parties

DATA EXPORTER

Name: [Insert CHS entity]
Address: [Insert CHS entity address]
Contact person's name, position, and contact details: [Insert details]
Activities relevant to the data transferred under the SCCs: As described in the Primary Agreement
Signature and date: See signatures and date(s) signed on signature page of the Addendum
Role: Controller

DATA IMPORTER
Name: [Insert service provider]
Address: [Insert service provider address]
Contact person's name, position, and contact details: [Insert details]
Activities relevant to the data transferred under the SCCs: As described in the Primary Agreement

Signature and date: See signatures and date(s) signed on signature page of the Addendum
Role: Processor

Part B. Description of transfer

Categories of data subjects whose Personal Data is transferred:
• [Insert details]

Categories of Personal Data transferred:
• [Insert details]

Categories of sensitive data including additional measures
• [Insert details if applicable or mark as N/A if not applicable].

ANEXO 1 A LAS CLÁUSULAS CONTRACTUALES TIPO DE LA UE

El presente Anexo 1 incluye ciertos detalles del Procesamiento de Datos Personales de CHS (CHS Inc.) según lo exige el Artículo 28(3) del RGPD (o según corresponda, disposiciones equivalentes de cualquier otra ley de protección de datos).

Parte A. Listado de las partes

EXPORTADOR DE DATOS

Nombre: [Insertar sociedad de CHS]
Domicilio: [Insertar domicilio de la Sociedad de CHS]
Nombre de la persona de contacto, cargo y datos de contacto: [Insertar detalles]
Actividades relevantes para los datos transferidos bajo las CCE: Tal como se describen en el Contrato Principal
Firma y fecha: Ver firmas y fecha(s) que figuran en la página de firmas de la Adenda
Cargo: Responsable

IMPORTADOR DE DATOS
Nombre: [Insertar el proveedor de servicios]
Domicilio: [Insertar el domicilio del proveedor de servicios]
Nombre de la persona de contacto, cargo y datos de contacto: [Insertar detalles]
Actividades relevantes para los datos transferidos bajo las CCE: Tal como se describen en el Contrato Principal
Firma y fecha: Ver firmas y fecha(s) que figuran en la página de firmas de la Adenda
Cargo: Encargado de Tratamiento

Parte B. Descripción de la transferencia

Categorías de titulares de datos cuyos Datos Personales se transfieren:
• [Insertar detalles]

Categorías de Datos Personales transferidos:
• [Insertar detalles]

Categorías de datos sensibles, incluidas medidas adicionales
• [Insertar detalles, si aplica, o indicar N/A si no aplica].

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

- Continuous

Nature of the Processing

- [Insert general description of the Processing Services to be provided.]

Purpose(s) of the data transfer and further Processing

- [Insert general description of the purposes for which the Personal Data will be Processed.]

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:

- *The Personal Data transferred may be stored in identifiable form for no longer than necessary for the purposes for which the Personal Data was transferred and, in no event, longer than permitted under the laws of the country of the data exporter.*

For transfers to (sub-) processors, provide a list of (sub-) processors:

- [Insert List or URL where list of (sub-) processors can be viewed]

For transfers to (sub-) processors, also specify subject matter, nature and duration of the Processing

- [Subject matter, nature and duration of Processing for transfers to (sub-)processor].

List country or countries where Data Importer or any of its sub-processors are Processing Personal Data.

- [Insert list]

Part C. Competent supervisory authority The competent supervisory authority is the supervisory authority of the EU/EEA Member State where the CHS data exporter is established. For data transfers under the FADP it is the Federal Data Protection and Information Commissioner.

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

- Continua

Naturaleza del Tratamiento

- [Insertar descripción general de los Servicios de Tratamiento a prestar.]

Finalidad(es) de la transferencia de datos y posterior Tratamiento

- [Insertar descripción general de las finalidades para las cuales serán tratados los Datos Personales.]

El período durante el cual se deberán conservar los Datos Personales o, si eso no fuera posible, los criterios utilizados para determinar dicho período:

- *Los Datos Personales transferidos se podrán almacenar en forma identificable en un tiempo no mayor al necesario para los fines para los cuales fueron transferidos y, en ningún caso, por un plazo mayor al permitido por las leyes del país del exportador de datos.*

Para transferencias a (sub)encargados, proporcionar una lista de (sub)encargados:

- [Insertar lista o URL donde se puede ver la lista de (sub)encargados]

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

- [Objeto, naturaleza y duración del Tratamiento para transferencias al (sub)encargado del tratamiento].

Listado el país o los países donde el Importador de Datos o cualquiera de sus subencargados están tratando Datos Personales.

- [Insertar listas]

Parte C. Autoridad de control competente La autoridad de control competente es la del Estado miembro de la UE/EEE donde esté establecido el exportador de datos CHS. Para las transferencias de datos en virtud del FADP, es el Comisionado Federal de Protección de Datos e Información.

ANNEX I - INFORMATION SECURITY REQUIREMENTS

Taking into account the nature, scope, context and purpose of the Processing, and the risks for the rights and freedoms of individuals, Supplier shall implement appropriate physical, technical, and organisational measures to ensure a level of security of CHS Personal Data appropriate to the risk, as follows:

1. **Information Security.**
   - **a.** Supplier will implement and maintain a written information security program including appropriate policies, procedures, and risk assessments that are reviewed at least annually.
   - **b.** Supplier will implement administrative, physical, and technical safeguards to:
     - i. Protect CHS Personal Data from unauthorized access, exfiltration, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage;
     - ii. Supplier will not utilize or store any CHS Personal Data in self-improving or machine learning software, models, algorithms, hardware or other tools or aids of any kind, and
     - iii. Take all necessary steps in mitigating damage, losses, costs and expenses caused by the events set forth in Section 4 of this Addendum.
   - **c.** Supplier shall notify CHS of any significant changes to administrative, physical, or technical safeguards, that could reasonably be expected to adversely affect the protection of CHS Personal Data from unauthorized access, exfiltration, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage.
   - **d.** All right, title and interest in CHS Personal Data will remain the property of CHS. Supplier has no intellectual property rights or other claim to CHS Personal Data that is hosted, stored, or transferred to and from Supplier's own systems and facilities or a third party hosted cloud provider. CHS Personal Data will not be used for analytics,

ANEXO I – REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta la naturaleza, el alcance, el contexto y la finalidad del Tratamiento, así como los riesgos para los derechos y libertades de las personas, el Proveedor deberá implementar medidas físicas, técnicas y organizativas apropiadas para garantizar un nivel de seguridad de los Datos Personales de CHS adecuado con el riesgo, de la siguiente manera:

1. **Seguridad de la información.**
   - **a.** El proveedor deberá implementar y mantener un programa de seguridad de la información escrito que incluya políticas, procedimientos y evaluaciones de riesgos apropiados que se revisen al menos una vez al año.
   - **b.** El Proveedor implementará medidas de protección administrativas, físicas y técnicas para:
     - i. Proteger los Datos Personales de CHS contra acceso no autorizado, exfiltración, adquisición o divulgación, destrucción, alteración, pérdida accidental, uso indebido o daño;
     - ii. El Proveedor no deberá utilizar ni almacenar ningún Dato Personal de CHS en software, modelos, algoritmos, hardware u otras herramientas o ayudas de ningún tipo, de automejora o aprendizaje automático, y
     - iii. Adoptar todas las medidas necesarias para mitigar los daños, pérdidas, costos y gastos causados por los eventos previstos en el Artículo 4 de este Anexo.
   - **c.** El Proveedor deberá notificar a CHS sobre cualquier cambio significativo en las medidas de protección administrativas, físicas o técnicas, que razonablemente se podría esperar que afecten negativamente la protección de los Datos Personales de CHS contra acceso no autorizado, exfiltración, adquisición o divulgación, destrucción, alteración, pérdida accidental, uso indebido o daño.
   - **d.** Todos los derechos, títulos e intereses sobre los Datos Personales de CHS seguirán siendo propiedad de CHS. El Proveedor no tendrá derechos de propiedad intelectual ni ningún otro reclamo sobre los Datos

marketing or anything outside of the intended use set out in this Agreement, or for the benefit of anyone other than CHS.

e. Where Supplier receives, stores and/or Processes CHS Personal Data using Supplier's own systems and facilities, or a third party hosted cloud provider, Supplier shall not change the location of CHS Personal Data or designated hosting provider without the authorization of the CHS. In the event that the Supplier, for any reason, requests to change the hosting region or hosting provider Supplier shall provide the CHS with notice at least sixty (60) days prior to any such change. CHS shall have the right to object to such requested change and/or terminate the Agreement and this Addendum at its sole discretion.

f. Where Supplier receives, stores, and/or Processes CHS Personal Data using Supplier's own systems and facilities, Supplier will implement, and maintain, CIS Critical Controls (defined as the then-current Center for Internet Security Critical Security Controls for Effective Cyber Defense), including, but not limited to, the following controls, each as is more fully explained in the CIS Critical Controls, as follows:

i. Inventory and Control of Enterprise Assets. Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

ii. Inventory of Authorized and Unauthorized Software. Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and ensure that

Personales de CHS alojados, almacenados o transferidos hacia y desde sus propios sistemas e instalaciones o de un proveedor de servicios en la nube externo. Los Datos Personales de CHS no se utilizarán con fines analíticos, de marketing ni para ningún otro fin distinto del previsto en este Contrato, ni para beneficio de terceros ajenos a CHS.

e. Cuando el Proveedor reciba, almacene o procese Datos Personales de CHS utilizando sus propios sistemas e instalaciones o los de un proveedor de nube alojado por un tercero, el Proveedor no deberá cambiar la ubicación de los Datos Personales de CHS ni al proveedor de alojamiento designado sin la autorización de CHS. En caso de que, por cualquier motivo, el Proveedor solicite un cambio de región o de proveedor de alojamiento, deberá notificar a CHS con al menos sesenta (60) días de antelación a dicho cambio. CHS tendrá derecho a oponerse a dicho cambio solicitado o a rescindir el Contrato y esta Adenda a su entera discreción.

f. Cuando el Proveedor reciba, almacene y/o procese Datos Personales CHS utilizando sus propios sistemas e instalaciones, el Proveedor implementará y mantendrá los Controles Críticos del CIS (definidos como los Controles Críticos de Seguridad del Centro de Seguridad de Internet para una Ciberdefensa efectiva vigentes en ese momento), incluyendo, sin limitación, los siguientes controles, cada uno de los cuales se explica con más detalle en los Controles Críticos del CIS, de la siguiente manera:

i. Inventario y control de activos empresariales. Gestionar activamente (inventariar, rastrear y corregir) todos los activos empresariales (dispositivos de usuario final, incluyendo portátiles y móviles; dispositivos de red; dispositivos no informáticos/de Internet de las Cosas (IoT); y servidores) conectados a la infraestructura física, virtual y remotamente, así como aquellos en entornos de nube, para conocer con precisión la totalidad de los activos que necesitan ser monitoreados y protegidos dentro de la empresa. Esto también facilitará la identificación de activos no autorizados y sin gestión para su eliminación o resolución.

unauthorized and unmanaged software is found and prevented from installation or execution.

iii. Secure Configuration of Enterprise Assets and Software. Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

iv. Continuous Vulnerability Management. Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

v. Audit Log Management. Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

vi. E-Mail and Web Browser Protections. Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and e-mail systems.

vii. Malware Defenses. Prevent and control the installation, spread, and execution of malicious applications, code or scrips on enterprise assets.

viii. Network Infrastructure Management. Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

ix. Data Recovery. Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

ii. Inventario de software autorizado y no autorizado. Gestionar activamente (inventariar, rastrear y corregir) todo el software en la red para que sólo se instale y pueda ejecutarse el software autorizado, y garantizar que se encuentre y se evite la instalación o ejecución de software no autorizado y no administrado.

iii. Configuración segura de activos y software empresariales. Establecer y mantener la configuración segura de los activos empresariales (dispositivos de usuario final, incluidos portátiles y móviles; dispositivos de red; dispositivos no informáticos/IoT; y servidores) y software (sistemas operativos y aplicaciones).

iv. Gestión Continua de Vulnerabilidades. Desarrollar un plan para evaluar y rastrear continuamente las vulnerabilidades en todos los activos de la infraestructura empresarial, con el fin de resolverlas y minimizar las oportunidades para los atacantes. Monitorear las fuentes públicas y privadas del sector para obtener nueva información sobre amenazas y vulnerabilidades.

v. Gestión de registros de auditoría. Recopilar, alertar, revisar y conservar registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.

vi. Protecciones de Correo electrónico y de Navegador Web. Minimizar la superficie de ataque y las oportunidades de que los atacantes manipulen el comportamiento humano a través de su interacción con navegadores web y sistemas de correo electrónico.

vii. Defensas contra Malware. Prevenir y controlar la instalación, propagación y ejecución de aplicaciones, códigos o scripts maliciosos en los activos empresariales.

viii. Gestión de la infraestructura de red. Establecer, implementar y administrar activamente (rastrear, informar, corregir) dispositivos de red, con el fin de evitar que los atacantes exploten servicios de red y puntos de acceso vulnerables.

x. Network Monitoring and Defense. Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

xi. Data Protection. Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

xii. Account Management. Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

xiii. Access Control Management. Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

xiv. Security Awareness and Skills Training. Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

xv. Application Software Security. Manage the security life cycle of all in-house developed, hosted and acquired software in order to prevent, detect, and remediate security weaknesses before they may impact the enterprise.

xvi. Incident Response Management. Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, communications) to prepare, detect, and quickly respond to an attack.

xvii. Penetration Testing. Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and

ix. Recuperación de Datos. Establecer y mantener prácticas de recuperación de datos suficientes para restaurar los activos empresariales dentro del alcance a un estado previo al incidente y confiable.

x. Monitoreo y defensa de la red. Operar procesos y herramientas para establecer y mantener un monitoreo y defensa integral de la red contra amenazas de seguridad en toda la infraestructura de red y la base de usuarios de la empresa.

xi. Protección de Datos. Desarrollar procesos y controles técnicos para identificar, clasificar, manejar de forma segura, retener y eliminar datos.

xii. Gestión de cuentas. Utilizar procesos y herramientas para asignar y administrar la autorización de credenciales para cuentas de usuario, incluidas cuentas de administrador, así como cuentas de servicio, para activos y software empresariales.

xiii. Gestión del control de acceso. Utilizar procesos y herramientas para crear, asignar, administrar y revocar credenciales de acceso y privilegios para cuentas de usuario, administrador y servicio para activos y software empresariales.

xiv. Concientización y capacitación en seguridad. Establecer y mantener un programa de concientización sobre seguridad para influir en el comportamiento de los trabajadores para que sean conscientes de la seguridad y estén debidamente capacitados para reducir los riesgos de ciberseguridad para la empresa.

xv. Seguridad de Software de Aplicaciones. Gestionar el ciclo de vida de seguridad de todo el software desarrollado, alojado y adquirido internamente para prevenir, detectar y solucionar las debilidades de seguridad antes de que puedan afectar a la empresa.

xvi. Gestión de respuesta a incidentes. Establecer un programa para desarrollar y mantener una capacidad de respuesta a incidentes (por ejemplo, políticas, planes, procedimientos, roles definidos, capacitación, comunicaciones) para

simulating the objectives and actions of an attacker.

xviii. Supplier Management. Develop a process to evaluate service providers who hold sensitive data or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

preparar, detectar y responder rápidamente a un ataque.

xvii. Prueba de Penetración. Poner a prueba la eficacia y la resiliencia de los activos empresariales identificando y explotando las debilidades en los controles (personas, procesos y tecnología) y simulando los objetivos y acciones de un atacante.

xviii. Gestión de proveedores. Desarrollar un proceso para evaluar a los proveedores de servicios que poseen datos confidenciales o son responsables de las plataformas o procesos de tecnología de información críticos de una empresa, para garantizar que estos proveedores protejan esas plataformas y datos de manera adecuada.

2. Audits

a. CHS shall treat any of the following or other audit reports as Supplier's confidential information for the purposes of confidentiality obligations, if any, under any then-existing agreement(s) between Supplier and the CHS. Supplier will promptly remedy any exception or failure noted in any industry standard independent audit report.

b. Supplier will, with respect to each system that holds, contains, or Processes CHS Personal Data:

i. Cause examinations to be performed by one or more qualified third parties as stated in, and contemplated by, a Service Organization Controls ("SOC") report or an industry standard independent audit report issued by such third party(ies) attesting to the Supplier management's description of Supplier's system fairly presents the system that was designed and implemented, at either a specific date not earlier than one year prior to the date of determination (in the case of a Type 1 report) or implemented throughout a specified time period that includes a date not earlier than one year prior to the date of determination (in the case of a Type 2 report); and

2. Auditorías

a. CHS deberá tratar cualquiera de los siguientes u otros informes de auditoría como información confidencial del Proveedor a efectos de las obligaciones de confidencialidad, si las hubiere, en virtud de cualquier acuerdo(s) vigente(s) entre el Proveedor y CHS. El Proveedor deberá subsanar de inmediato cualquier excepción o incumplimiento detectado en cualquier informe de auditoría independiente estándar del sector.

b. El Proveedor, con respecto a cada sistema que contenga o procese Datos Personales de CHS, deberá:

i. Solicitar que uno o más terceros calificados realicen inspecciones, según lo estipulado y contemplado en un informe de Controles de la Organización de Servicios ("SOC") o en un informe de auditoría independiente estándar del sector emitido por dicho(s) tercero(s), que acredite que la descripción del sistema del Proveedor, realizada por la gerencia, presenta fielmente el sistema diseñado e implementado, ya sea en una fecha específica no anterior a un año antes de la fecha de determinación (en el caso de un informe de Tipo 1) o implementada durante un período específico que incluya una fecha no anterior a un año antes de la fecha de determinación (en el caso de un informe de Tipo 2); y

ii. For so long as such system holds, contains, or Processes CHS Personal Data, cause the system to conform in all material respects with management's assertions with respect to the system upon which the then-most-recent SOC report or an industry standard independent audit report, and bridge or gap letter which covers the period between the expiry of the previous report and the release of the new report.

c. Suppliers will, upon CHS's request, make available to CHS for review, as applicable, Supplier's latest Payment Card Industry ("PCI") Compliance Report, SOC audit report, or any industry standard independent audit reports or certifications performed by or on behalf of Supplier assessing the effectiveness of Supplier's information security program as relevant to the CHS Personal Data.

i. SOX: If Supplier is in scope for CHS's compliance with the Sarbanes–Oxley Act (the "SOX Act"), as may be amended from time to time, Supplier will provide annually to CHS, for review, Supplier's latest SOC report for as long as the system holds, contains or Processes CHS Personal Data, or

ii. PCI: Supplier will provide annually to CHS, for review, Supplier's latest PCI Compliance Report(s) and/or SOC report for as long as the system holds, contains or Processes CHS Personal Data.

d. Upon CHS's request, to confirm Supplier's compliance with this Addendum and any applicable laws, regulations, and industry standards, Supplier will permit CHS or CHS's agents to perform an assessment, audit, examination, or review of all controls in Supplier's physical and/or technical environment in relation to all CHS Personal Data being handled, received or acquired and/or services being provided to CHS under the Privacy Agreement and this Addendum. Supplier shall cooperate fully with such assessment by providing access to knowledgeable personnel, physical premises, documentation,

ii. Mientras dicho sistema mantenga, contenga o procese Datos Personales de CHS, hacer que el sistema se ajuste en todos los aspectos materiales a las afirmaciones de la gerencia con respecto al sistema en el que se basa el informe SOC más reciente o un informe de auditoría independiente estándar de la industria, y una carta puente o de brecha que cubra el período entre el vencimiento del informe anterior y la publicación del nuevo informe.

c. Los proveedores, a solicitud de CHS, pondrán a disposición de CHS para su revisión, según corresponda, el último Informe de Cumplimiento de la Industria de Tarjetas de Pago ("PCI") del Proveedor, el informe de auditoría de SOC o cualquier informe o certificación de auditoría independiente estándar de la industria realizado por o en nombre del Proveedor que evalúe la eficacia del programa de seguridad de la información del Proveedor en lo que respecta a los Datos Personales de CHS.

i. SOX: Si el Proveedor está dentro del alcance del cumplimiento de CHS con la Ley Sarbanes-Oxley (la "Ley SOX"), según pueda modificarse oportunamente, el Proveedor proporcionará en forma anual a CHS, para su revisión, el último informe SOC del Proveedor mientras el sistema tenga, contenga o procese Datos Personales de CHS, o

ii. PCI: El Proveedor proporcionará anualmente a CHS, para su revisión, los últimos Informes de Cumplimiento de PCI y/o el informe SOC mientras el sistema contenga o procese los Datos Personales de CHS.

d. A solicitud de CHS, para confirmar el cumplimiento del Proveedor con esta Adenda y cualquier ley, reglamentación y norma de la industria aplicable, el Proveedor permitirá a CHS o a los agentes de CHS realizar una evaluación, auditoría, examen o revisión de todos los controles en el entorno físico y/o técnico del Proveedor en relación con todos los Datos Personales de CHS que se manejan, reciben o adquieren y/o los servicios que se prestan a CHS en virtud del Acuerdo de Privacidad y esta Adenda. El Proveedor cooperará plenamente con dicha

infrastructure, and applicable software that Processes, stores, or transports the CHS Personal Data for CHS pursuant to the applicable agreement and this Addendum. In addition, upon CHS's request, Supplier shall provide CHS with the results of any audit by or on behalf of Supplier performed that assess the effectiveness of Supplier's information security program as relevant to the security and confidentiality of the CHS Personal Data shared during the course of the applicable agreement and this Addendum.

e. PCI DSS.

i. Definitions.

1. "Cardholder Data" has the meaning given to that term by the PCI DSS or any successor standard.
2. "PCI DSS" means the then-current Payment Card Industry Data Security Standard as promulgated by the PCI Security Standards Council.
3. "PCI Supplier" means a PCIservice provider as defined by PCI DSS.
4. "AOC" means the PCI Security Standard Council form for merchants and service providers to attest to the results of a PCI DSS assessment.;

ii. If, and to the extent that, any of the CHS Personal Data is Cardholder Data that Supplier receives or Processes as a PCI Supplier, Supplier will, unless expressly permitted otherwise in writing by the CHS:

iii. Maintain current assessments and all other qualifications and certifications necessary to that designation under PCI DSS;

iv. Deliver to CHS Supplier's AOC promptly upon completion thereof, in such form and containing such information as required under PCIDSS, dated not more than one year after the previous AOC (if any) delivered by Supplier to CHS;

v. Provide to CHS an agreed upon responsibility matrix identifying

evaluación proporcionando acceso a personal experto, instalaciones físicas, documentación, infraestructura y software aplicable que trata, almacena o transporta los Datos Personales de CHS para CHS de conformidad con el acuerdo aplicable y esta Adenda. Además, a solicitud de CHS, el Proveedor proporcionará a CHS los resultados de cualquier auditoría realizada por o en nombre del Proveedor que evalúe la eficacia del programa de seguridad de la información del Proveedor en lo que respecta a la seguridad y confidencialidad de los Datos Personales de CHS compartidos durante el curso del acuerdo aplicable y esta Adenda.

e. PCI DSS.

i. Definiciones.

1. "Datos del titular de la tarjeta" tiene el significado que le da a ese término el PCI DSS o cualquier norma que lo suceda.
2. "PCI DSS" significa la Norma de Seguridad de Datos de la Industria de Tarjetas de Pago vigente en ese momento, promulgado por el Consejo de Normas de Seguridad PCI.
3. "Proveedor de PCI" significa un proveedor de servicios PCI según lo define el PCI DSS.
4. "AOC" significa el formulario del Consejo de Normas de Seguridad PCI para que los comerciantes y proveedores de servicios den fe de los resultados de una evaluación PCI DSS.;

ii. Siempre que, y en la medida en que cualquiera de los Datos Personales de CHS sean Datos del Titular de la Tarjeta que el Proveedor recibe o trata como Proveedor de PCI, el Proveedor deberá, salvo expresa autorización por escrito de CHS:

iii. Mantener evaluaciones actualizadas y todas las demás calificaciones y certificaciones necesarias para dicha designación bajo PCI DSS;

iv. Entregar a CHS el AOC del Proveedor inmediatamente después de su finalización, en el formato y que contenga la información requerida según PCIDSS, con fecha no mayor a un año posterior al AOC anterior (si lo hubiera) entregado por el Proveedor a CHS;

which PCI DSS requirements will be managed by the Supplier; and

vi. Otherwise comply with all requirements of PCI DSS with respect to the Cardholder Data.

3. Access to CHS Information Systems

a. Use of Permitted Systems. Supplier will use any Permitted Systems solely to carry out Supplier's obligations to the CHS. Supplier will use Permitted Systems for no other purpose.

b. Conditions of Use. Supplier will use the Permitted Systems solely in accordance with the terms of such agreement(s) then in place between CHS and Supplier and such further conditions and policies as CHS makes available to Supplier from time to time. Such conditions and policies of use may include (and be described as) policies, procedures, technical requirements, and/or protocols. CHS may monitor authorized Supplier's personnel access and activities within CHS Permitted Systems.

c. Access by Authorized Supplier Personnel. Supplier will limit access to the Permitted Systems to authorized Supplier personnel. Supplier will provide to CHS the name of each authorized Supplier personnel. Each authorized Supplier personnel must establish and maintain a unique identifier for access and follow the same security rules as CHS personnel. Supplier shall ensure that individuals other than authorized Supplier personnel (including, without limitation, past employees and current employees who do not have an active role in providing goods, services, or software to CHS or CHS Affiliates) shall have no access to CHS Information Systems. Supplier shall remain responsible for all actions and inactions of such authorized Supplier personnel.

d. Specific Prohibitions. Except as expressly authorized by CHS in a signed writing (whether in a statement of work, project specification, work order, or separate written direction) Supplier shall not (i) attempt to reverse engineer, disassemble, reverse translate,

v. Proporcionar a CHS una matriz de responsabilidad acordada que identifique qué requisitos de PCI DSS serán gestionados por el Proveedor; y

vi. Cumplir de cualquier otro modo con todos los requisitos de PCI DSS con respecto a los Datos del Titular de la Tarjeta.

3. Acceso a los Sistemas de Información de CHS

a. Uso de Sistemas Permitidos. El Proveedor utilizará los Sistemas Permitidos únicamente para cumplir con sus obligaciones con CHS. El Proveedor no utilizará los Sistemas Permitidos para ningún otro propósito.

b. Condiciones de Uso. El Proveedor utilizará los Sistemas Permitidos únicamente de conformidad con los términos del contrato vigente entre CHS y el Proveedor, así como con las condiciones y políticas adicionales que CHS ponga a disposición del Proveedor periódicamente. Dichas condiciones y políticas de uso pueden incluir (y describirse como) políticas, procedimientos, requisitos técnicos y/o protocolos. CHS podrá supervisar el acceso y las actividades del personal autorizado del Proveedor dentro de los Sistemas Permitidos de CHS.

c. Acceso por parte del Personal del Proveedor Autorizado. El Proveedor deberá limitar el acceso a los Sistemas Permitidos a su personal autorizado. El Proveedor deberá proporcionar a CHS el nombre de cada miembro autorizado del personal. Cada miembro autorizado del personal del Proveedor deberá establecer y mantener un identificador único de acceso y seguir las mismas normas de seguridad que el personal de CHS. El Proveedor garantizará que las personas que no sean miembros autorizados del Proveedor (incluyendo, sin limitación, empleados anteriores y actuales que no participen activamente en la provisión de bienes, servicios o software a CHS o a las Empresas Vinculadas de CHS) no tengan acceso a los Sistemas de Información de CHS. El Proveedor será responsable de todas las acciones e inacciones de dicho personal autorizado.

d. Prohibiciones Específicas. Salvo que CHS lo autorice expresamente por escrito y firmado (ya sea en una declaración de trabajo, especificación del proyecto, orden de trabajo

decompile, or in any other manner decode any element of the CHS Information Systems; (ii) attempt to decrypt encrypted or scrambled information; (iii) make modifications, enhancements, adaptations or translations, in whole or in part, to or of any element of the CHS Information Systems, not authorized by CHS; (iv) access any CHS Information System in excess of the permission expressly granted by the CHS; (v) make copies of any element of the CHS Information Systems; (vi) use any CHS Information System or data to build a competitive product or service, or otherwise for commercial purposes; (vii) probe host computers or networks; (viii) breach or examine the security controls of a host computer, network component or authentication system, or circumvent or disclose CHS Information System user authentication or security controls; (ix) monitor data on any network or system without CHS's written authorization; (x) interfere with or disrupt the service of any user, host or network, or overload a server, network connected device, or network component or otherwise threaten harm to property; (xi) originate malformed data or network traffic that results in damage to, or disruption of, a service or network connected device; (xii) forge data or misrepresent the origination of a user or source; (xiii) take any action that is unlawful, abusive, malicious, harassing, tortious, defamatory, libelous or invasive of another's privacy right or infringing the IP rights of any person; (xiv) otherwise violate any applicable law or regulation; (xv) permit access by a competitor of CHS. Should an authorized Supplier personnel take any action in violation of this section, CHS may require Supplier to replace the authorized Supplier personnel with another authorized Supplier personnel or suspend or terminate the Primary Agreement, statement of work, or order in its sole discretion, while preserving any other remedy available to CHS.

e. Failure of Access. Supplier acknowledges that access to the Permitted Systems may be interrupted

o instrucción escrita en forma separada), el Proveedor no deberá (i) intentar realizar ingeniería inversa, desensamblar, traducir de forma inversa, descompilar ni decodificar de ninguna otra manera ningún elemento de los Sistemas de información de CHS; (ii) intentar descifrar información cifrada o codificada; (iii) realizar modificaciones, mejoras, adaptaciones o traducciones, totales o parciales, a ningún elemento de los Sistemas de información de CHS, sin la autorización de CHS; (iv) acceder a ningún Sistema de información de CHS sin el permiso expresamente otorgado por CHS; (v) realizar copias de ningún elemento de los Sistemas de información de CHS; (vi) utilizar ningún Sistema de información o datos de CHS para crear un producto o servicio competitivo ni, de otro modo, con fines comerciales; (vii) sondear computadoras host o redes; (viii) violar o examinar los controles de seguridad de una computadora host, un componente de red o un sistema de autenticación, ni eludir o revelar los controles de seguridad o autenticación de usuarios del Sistema de información de CHS; (ix) monitorear datos en cualquier red o sistema sin la autorización escrita de CHS; (x) interferir o interrumpir el servicio de cualquier usuario, host o red, o sobrecargar un servidor, dispositivo conectado a la red o componente de red o de otra manera amenazar con dañar la propiedad; (xi) originar datos malformados o tráfico de red que resulte en daño o interrupción de un servicio o dispositivo conectado a la red; (xii) falsificar datos o tergiversar el origen de un usuario o fuente; (xiii) realizar cualquier acción que sea ilegal, abusiva, maliciosa, acosadora, ilícita, difamatoria, calumniosa o invasiva del derecho a la privacidad de otro o que infrinja los derechos de propiedad intelectual de cualquier persona; (xiv) de otra manera incumplir cualquier ley o reglamentación aplicable; (xv) permitir el acceso de un competidor de CHS. Si un miembro del personal autorizado del Proveedor realiza alguna acción que incumpla este artículo, CHS podrá exigir al Proveedor que reemplace al miembro del personal autorizado del Proveedor con otro miembro del personal autorizado del Proveedor o que suspenda o rescinda el Contrato Principal, la declaración de trabajo o la orden a su

due to circumstances within or outside the reasonable control of the CHS. Nothing in this Addendum or any agreement between Supplier and CHS will be a promise or covenant to deliver access to the Permitted Systems or that any Permitted System will be functional. Aside from the access as provided under this Addendum, no license under any patent, copyright, or any other intellectual property right in respect of CHS Information System is granted to Supplier by virtue of access to the Permitted Systems.

f. Waiver of Liability. CHS excludes all representations, warranties, and covenants, express or implied, by CHS or CHS Affiliates with respect to the CHS Information Systems, including, but not limited to, any representations, warranties, or conditions of accuracy, sufficiency, suitability, or non-infringement regarding Supplier's access to, or use of, any Permitted System. CHS will have no liability whatsoever for any damages, losses, or expenses incurred by Supplier as a result of Supplier's or its authorized Supplier personnel's access to the Permitted Systems (including, without limitation, the inadvertent accessing of a computer virus or other harmful computer file or program), or of failure of the Permitted System(s) to be available or accessible.

g. Supplier Systems. Where Supplier accesses Permitted Systems using Supplier's hardware, software, or networks, the following provisions will apply.

i. Access Security. Supplier shall ensure that authorized Supplier personnel obtain access to the Permitted Systems through a computer system that maintains authentication controls and includes a suitable firewall. Supplier shall follow all of CHS's security rules and procedures for restricting access to its computer systems.

ii. Segregation Wall. Supplier will ensure that authorized Supplier personnel are effectively isolated from its personnel who are assigned to the account of a known

exclusivo criterio, mientras preserva cualquier otro recurso disponible para CHS.

e. Falla de Acceso. El Proveedor reconoce que el acceso a los Sistemas Permitidos puede verse interrumpido por circunstancias, dentro o fuera del control razonable de CHS. Ninguna de las disposiciones de esta Adenda ni de ningún acuerdo entre el Proveedor y CHS constituirá una promesa o compromiso de proporcionar acceso a los Sistemas Permitidos ni de garantizar su funcionamiento. Más allá del acceso previsto en esta Adenda, no se concede al Proveedor ninguna licencia de patente, derecho de autor ni ningún otro derecho de propiedad intelectual sobre el Sistema de Información de CHS por el acceso a los Sistemas Permitidos.

f. Renuncia de Responsabilidad. CHS excluye todas las declaraciones, garantías y convenios, explícitos o implícitos, de CHS o las Empresas Vinculadas de CHS con respecto a los Sistemas de Información de CHS, incluyendo, entre otros, cualquier declaración, garantía o condición de exactitud, suficiencia, idoneidad o no infracción en relación con el acceso o uso del Proveedor a cualquier Sistema Permitido. CHS no será responsable de daños y perjuicios, pérdida o gasto alguno en que incurra el Proveedor como resultado del acceso del Proveedor o de su personal autorizado a los Sistemas Permitidos (incluyendo, entre otros, el acceso involuntario a un virus informático u otro archivo o programa informático dañino), o de la falta de disponibilidad o acceso al/a los Sistema(s) Permitido(s).

g. Sistemas del Proveedor. Cuando el Proveedor acceda a los Sistemas Permitidos utilizando hardware, software o redes del Proveedor, aplicarán las siguientes disposiciones.

i. Seguridad de Acceso. El Proveedor deberá garantizar que su personal autorizado acceda a los Sistemas Permitidos mediante un sistema informático con controles de autenticación e incluido un cortafuegos adecuado. El Proveedor deberá cumplir con todas las normas y procedimientos de seguridad de CHS para restringir el acceso a sus sistemas informáticos.

or potential competitor of CHS or CHS Affiliates. Supplier will establish and document physical and electronic procedures to segregate and protect all information, data and communications (including, but not limited to, CHS Personal Data).

ii. Muro de Segregación. El Proveedor deberá garantizar que su personal autorizado esté eficazmente aislado del personal asignado a la cuenta de un competidor conocido o potencial de CHS o de las Empresas Vinculadas de CHS. El Proveedor deberá establecer y documentar procedimientos físicos y electrónicos para separar y proteger toda la información, los datos y las comunicaciones (incluyendo, sin limitación, los Datos Personales de CHS).

iii. ANNEX II – BRAZILIAN MODEL CLAUSES

CLAUSE 1. Identification of the Parties

1.1. By this agreement, the Exporter and the Importer (hereinafter, "Parties"), identified below, have agreed to these standard contractual clauses (hereinafter, "Clauses") approved by the National Data Protection Authority (ANPD), to govern the International Data Transfer described in CLAUSE 2, in accordance with the provisions of the National Legislation.

Name: Qualification: [CHS Entity]
Main Address:
E-mail Address:
Contact for the Data Subject:
Other information:

(x) Exporter/Controller

Name: Qualification:
Main Address:
E-mail Address:
Contact for the Data Subject:
Other information:

(x) Importer/Processor

CLAUSE 2. Object

2.1 This Clauses shall apply to International Transfers of Personal Data between Data Exporters and Data Importers, as described below.

Description of the international data transfer:

Main purposes of the transfer:
Categories of personal data transferred:
Period of data storage:
Other information:

iii. ANEXO II – CLÁUSULAS MODELO BRASILEÑAS

CLÁUSULA 1. Identificación de las Partes

1.1. Mediante el presente acuerdo, el Exportador y el Importador (en adelante, las «Partes»), identificados a continuación, han acordado las presentes cláusulas contractuales tipo (en adelante, las «Cláusulas»), aprobadas por la Autoridad Nacional de Protección de Datos (ANPD), para regir la Transferencia Internacional de Datos descripta en la CLÁUSULA 2, de conformidad con lo dispuesto en la legislación nacional.

Nombre: Calificación: [Sociedad de CHS]
Domicilio principal:
Dirección de correo electrónico:
Contacto para el Titular de Datos:
Otra información:

(x) Exportador/Responsable

Nombre: Calificación:
Domicilio principal:
Dirección de correo electrónico:
Contacto para el Titular de Datos:
Otra información:

(x) Importador/Encargado de tratamiento

CLÁUSULA 2. Objeto

2.1 Estas Cláusulas se aplicarán a las Transferencias Internacionales de Datos Personales entre Exportadores de Datos e Importadores de Datos, como se describe a continuación.

Descripción de la transferencia internacional de datos:

Finalidades principales de la transferencia:
Categorías de datos personales transferidos:
Periodo de conservación de los datos:
Otra información:

CLAÚSU 3. Onward Transfers

OPTION A. 3.1. The Importer may not carry out an Onward Transfer of Personal Data subject to the International Data Transfer governed by these Clauses, except in the cases provided for in item 18.3.

OPTION B. 3.1. The Importer may carry out an Onward Transfer of Personal Data subject to the International Data Transfer governed by these Clauses, in the cases and according to the conditions described below and the provisions of CLAUSE 18.

Main purposes of the transfer:
Categories of personal data transferred:
Period of data storage:
Other information:

CLAUSE 4. Responsibilities of the Parties

4.1 Without prejudice to the duty of mutual assistance and the general obligations of the Parties, the Designated Party below, as Controller, shall be responsible for complying with the following obligations set out in these Clauses:

a) Responsible for publishing the document provided in CLAUSE 14:

( ) Exporter ( ) Importer

b) Responsible for responding to requests from Data Subjects dealt with in CLAUSE 15:

( ) Exporter ( ) Importer

c) Responsible for notifying the security incident provided in CLAUSE 16:

( ) Exporter ( ) Importer

4.2. For the purposes of these Clauses, if the Designated Party pursuant to item 4.1. is the Processor, the Controller remains responsible for:

CLÁUSULA 3. Transferencias posteriores

OPCIÓN A. 3.1. El Importador no podrá realizar una Transferencia Posterior de Datos Personales sujeta a la Transferencia Internacional de Datos regida por estas Cláusulas, salvo en los casos previstos en el punto 18.3.

OPCIÓN B. 3.1. El Importador podrá realizar una Transferencia Posterior de Datos Personales sujeta a la Transferencia Internacional de Datos regida por estas Cláusulas, en los casos y según las condiciones descriptas a continuación y lo dispuesto en la CLÁUSULA 18.

Finalidades principales de la transferencia:
Categorías de datos personales transferidos:
Periodo de conservación de los datos:
Otra información:

CLÁUSULA 4. Responsabilidades de las Partes

4.1 Sin perjuicio del deber de asistencia mutua y de las obligaciones generales de las Partes, la Parte Designada a continuación, en su calidad de Responsable, será responsable de cumplir con las siguientes obligaciones establecidas en estas Cláusulas.:

a) Responsable de publicar el documento previsto en la CLÁUSULA 14:

( ) Exportador ( ) Importador

b) Responsable de responder las solicitudes de los Titulares de Datos previstos en la CLÁUSULA 15:

( ) Exportador ( ) Importador

c) Responsable de notificar el incidente de seguridad previsto en la CLÁUSULA 16:

( ) Exportador ( ) Importador

4.2. A los efectos de estas Cláusulas, si la Parte Designada de conformidad con el punto 4.1. es el Encargado del Tratamiento, el Responsable sigue siendo responsable de:

a) compliance with the obligations provided in CLAUSES 14, 15 and 16 and other provisions established in the National Legislation, especially in case of omission or non-compliance with the obligations by the Designated Party;
b) compliance with ANPD's determinations; and
c) guaranteeing the Data Subjects' rights and repairing damages caused, subject to the provisions of Clause 17.

SECTION II – MANDATORY CLAUSES

CLAUSE 5 Purpose

5.1 These Clauses are presented as a mechanism to enable the secure international flow of personal data, establish minimum guarantees and valid conditions for carrying out the International Data Transfer and aim to guarantee the adoption of adequate safeguards for compliance with the principles, the rights of the Data Subject and the data protection regime provided for in National Legislation.

CLAUSE 6. Definitions

6.1 For the purposes of these Clauses, the definitions in art. 5 of LGPD, and art. 3 of the Regulation on the International Transfer of Personal Data shall be considered, without prejudice to other normative acts issued by ANPD. The Parties also agree to consider the terms and their respective meanings as set out below:

a) Processing agents: the controller and the processor;
b) ANPD: National Data Protection Authority;
c) Clauses: the standard contractual clauses approved by ANPD, which are part of SECTIONS I, II and III;
d) Related Contract: contractual instrument signed between the Parties or, at least, between one of them and a third-party, including a Third-Party Controller, which has a common purpose, link or dependency relationship with the contract that governs the International Data Transfer;
e) Controller: Party or third-party ("Third Controller") responsible for decisions regarding the processing of Personal Data;

a) el cumplimiento de las obligaciones previstas en las CLÁUSULAS 14, 15 y 16 y demás disposiciones establecidas en la Legislación Nacional, especialmente en caso de omisión o incumplimiento de las obligaciones por parte de la Parte Designada;
b) el cumplimiento de las determinaciones de la ANPD; y
c) garantizar los derechos de los Titulares de los Datos y reparar los daños causados, sujeto a lo dispuesto en la Cláusula 17.

SECCIÓN II – CLÁUSULAS OBLIGATORIAS

CLÁUSULA 5 Propósito

5.1 Estas Cláusulas se presentan como un mecanismo para posibilitar el flujo internacional seguro de datos personales, establecen garantías mínimas y condiciones válidas para llevar a cabo la Transferencia Internacional de Datos y tienen como objetivo garantizar la adopción de medidas de protección adecuadas para el cumplimiento de los principios, los derechos del Titular de los Datos y el régimen de protección de datos previsto en la Legislación Nacional.

CLÁUSULA 6. Definiciones

6.1 A los efectos de estas Cláusulas, se considerarán las definiciones del art. 5 de la LGPD y del art. 3 del Reglamento sobre la Transferencia Internacional de Datos Personales, sin perjuicio de otras normas emitidas por la ANPD. Las Partes también acuerdan considerar los términos y sus respectivos significados, tal como se establece a continuación.:

a) Agentes del tratamiento: el responsable y el encargado del tratamiento;
b) ANPD: Autoridad Nacional de Protección de Datos;
c) Cláusulas: las cláusulas contractuales tipo aprobadas por la ANPD, que forman parte de los SECCIONES I, II y III;
d) Contrato Relacionado: instrumento contractual suscrito entre las Partes o, al menos, entre una de ellas y un tercero, incluido un Responsable Tercero, que tenga un propósito común, vínculo o relación de dependencia con el contrato que rige la Transferencia Internacional de Datos;
e) Responsable: Parte o tercero ("Tercero Responsable") responsable de las decisiones relativas al tratamiento de Datos Personales;

f) Personal Data: information related to an identified or identifiable natural person;
g) Sensitive Personal Data: personal data on racial or ethnic origin, religious belief, political opinion, affiliation to trade unions or to a religious, philosophical or political organization, data regarding health or sexual life, genetic or biometric data, whenever related to a natural person;
h) Erasure: exclusion of data or dataset from a database, regardless of the procedure used;
i) Exporter: processing agent, located in the national territory or in a foreign country, who transfers personal data to the Importer;
j) Importer: processing agent, located in a foreign country, who receives personal data from the Exporter;
k) National Legislation: set of Brazilian constitutional, legal and regulatory provisions regarding the protection of Personal Data, including the LGPD, the International Data Transfer Regulation and other normative acts issued by ANPD;
l) Arbitration Law: Law No. 9,307, of September 23, 1996;
m) Security Measures: technical and administrative measures able to protect Personal Data from unauthorized access and from accidental or unlawful events of destruction, loss, alteration, communication or dissemination;
n) Research Body: body or entity of the government bodies or associated entities or a non-profit private legal entity legally established under Brazilian laws, having their headquarter and jurisdiction in the Brazilian territory, which includes basic or applied research of historical, scientific, technological or statistical nature in its institutional mission or in its corporate or statutory purposes;
o) Processor: Party or third-party, including a Sub-processor, which processes Personal Data on behalf of the Controller;
p) Designated Party: Party or a Third-Party Controller, under the terms of CLAUSE 4, designated to fulfill specific obligations regarding transparency, Data Subjects' rights and notifying security incidents;
q) Parties: Exporter and Importer;
r) Access Request: request for mandatory compliance, by force of law, regulation or determination of public authority, to grant

f) Datos Personales: información relativa a una persona física identificada o identificable;
g) Datos Personales Sensibles: datos personales sobre el origen racial o étnico, las creencias religiosas, las opiniones políticas, la afiliación a sindicatos o a una organización religiosa, filosófica o política, datos relativos a la salud o a la vida sexual, datos genéticos o biométricos, siempre que se refieran a una persona física;
h) Supresión: exclusión de un dato o conjunto de datos de una base de datos, independientemente del procedimiento utilizado.;
i) Exportador: agente de tratamiento, ubicado en territorio nacional o en país extranjero, que transfiere datos personales al Importador;
j) Importador: agente encargado de tratamiento, ubicado en un país extranjero, que recibe datos personales del Exportador;
k) Legislación Nacional: conjunto de disposiciones constitucionales, legales y reglamentarias brasileñas relativas a la protección de Datos Personales, incluyendo la LGPD, el Reglamento de Transferencia Internacional de Datos y otros actos normativos emitidos por la ANPD;
l) Ley de Arbitraje: Ley Nº 9.307, de 23 de septiembre de 1996;
m) Medidas de Seguridad: medidas técnicas y administrativas capaces de proteger los Datos Personales de accesos no autorizados y de eventos accidentales o ilícitos de destrucción, pérdida, alteración, comunicación o difusión;
n) Organismo de Investigación: organismo o entidad de los órganos gubernamentales o entidades asociadas o persona jurídica privada sin fines de lucro legalmente constituida bajo las leyes brasileñas, que tenga su sede y jurisdicción en el territorio brasileño, que incluya investigación básica o aplicada de naturaleza histórica, científica, tecnológica o estadística en su misión institucional o en sus fines corporativos o estatutarios.;
o) Encargado del Tratamiento: Parte o tercero, incluido un Subencargado del Tratamiento, que trata Datos Personales por cuenta del Responsable del Tratamiento;
p) Parte Designada: Parte o un Tercero Responsable del Tratamiento, en los términos de la CLÁUSULA 4, designado para cumplir obligaciones específicas en materia de transparencia, derechos de los Titulares de los Datos y notificación de incidentes de seguridad.;

access to the Personal Data subject to the International Data Transfer governed by these Clauses;

s) Sub-processor: processing agent hired by the Importer, with no link with the Exporter, to process Personal Data after an International Data Transfer;
t) Data Subject: natural person to whom the Personal Data which are subject to the International Data Transfer governed by these Clauses relate;
u) Transfer: processing modality through which a processing agent transmits, shares or provides access to Personal Data to another processing agent;
v) International Data Transfer: transfer of Personal Data to a foreign country or to an international organization which Brazil is a member of; and
w) Onward Transfer: transfer of Personal Data, within the same country or to another country, by an Importer to a third-party, including a Sub-processor, provided that it does not constitute an Access Request.

q) Partes: Exportador e Importador;
r) Solicitud de Acceso: solicitud de cumplimiento obligatorio, por fuerza de ley, regulación o determinación de autoridad pública, para conceder acceso a los Datos Personales objeto de la Transferencia Internacional de Datos regulada por estas Cláusulas.;
s) Subencargado del tratamiento: agente de tratamiento contratado por el Importador, sin vínculo con el Exportador, para tratar Datos Personales tras una Transferencia Internacional de Datos;
t) Titular de los Datos: persona física a la que se refieren los Datos Personales que sean objeto de la Transferencia Internacional de Datos regida por las presentes Cláusulas;
u) Transferencia: modalidad de tratamiento mediante la cual un encargado del tratamiento transmite, comparte o proporciona acceso a Datos Personales a otro encargado del tratamiento;
v) Transferencia Internacional de Datos: transferencia de Datos Personales a un país extranjero o a una organización internacional de la que Brasil sea miembro; y
w) Transferencia posterior: transferencia de Datos Personales, dentro del mismo país o a otro país, por un Importador a un tercero, incluido un Subencargado, siempre que no constituya una Solicitud de Acceso.

CLAUSE 7. Applicable legislation and ANPD supervision

7.1. The International Data Transfer subject to these Clauses shall subject to the National Legislation and to the supervision of ANPD, including the power to apply preventive measures and administrative sanctions to both Parties, as appropriate, as well as the power to limit, suspend or prohibit the international transfers arising from this agreement or a Related Contract.

CLAÚSULA 7. Legislación aplicable y supervisión de la ANPD

7.1. La Transferencia Internacional de Datos sujeta a estas Cláusulas estará sujeta a la Legislación Nacional y a la supervisión de la ANPD, incluyendo la facultad de aplicar medidas preventivas y sanciones administrativas a ambas Partes, según corresponda, así como la facultad de limitar, suspender o prohibir las transferencias internacionales derivadas de este acuerdo o de un Contrato Relacionado.

CLAUSE 8. Interpretation

8.1. Any application of these Clauses shall occur in accordance with the following terms:

a) these Clauses shall always be interpreted more favorably to the Data Subject and in accordance with the provisions of the National Legislation;
b) in case of doubt about the meaning of any term in these Clauses, the meaning which

CLAÚSULA 8. Interpretación

8.1. Cualquier aplicación de estas Cláusulas se realizará de conformidad con los siguientes términos:

a) las presentes Cláusulas se interpretarán siempre de forma más favorable al Titular de los Datos y de conformidad con lo dispuesto en la Legislación Nacional;
b) en caso de duda sobre el significado de cualquier término en estas Cláusulas, se

is most in line with the National Legislation shall apply;
c) no item in these Clauses, including a Related Agreement and the provisions set forth in SECTION IV, shall be interpreted as limiting or excluding the liability of any of the Parties in relation to obligations set forth in the National Legislation; and
d) provisions of SECTIONS I and II shall prevail in case of conflict of interpretation with additional clauses and other provisions set forth in SECTIONS III and IV of this agreement or in Related Agreements.

aplicará el significado que más se ajuste a la Legislación Nacional;
c) ningún punto de estas Cláusulas, incluyendo un Contrato Relacionado y las disposiciones establecidas en la SECCIÓN IV, se interpretará como limitante o excluyente de la responsabilidad de cualquiera de las Partes en relación con las obligaciones establecidas en la Legislación Nacional; y
d) las disposiciones de las SECCIONES I y II prevalecerán en caso de conflicto de interpretación con cláusulas adicionales y demás disposiciones establecidas en las SECCIONES III y IV de este acuerdo o en Contratos Relacionados.

CLAUSE 9. Docking Clause

9.1. By mutual agreement between the Parties, it shall be possible for a processing agent to adhere to these Clauses, either as a Data Exporter or as a Data Importer, by completing and signing a written document, which shall form part of this contract.

9.2 The acceding party shall have the same rights and obligations as the originating parties, according to the position assumed of Exporter or Importer and according to the corresponding category of treatment agent.

CLÁUSULA 9. Cláusula de Incorporación

9.1. De mutuo acuerdo entre las Partes, será posible que un agente de procesamiento adhiera a estas Cláusulas, ya sea como Exportador de Datos o como Importador de Datos, completando y firmando un documento escrito, que formará parte de este contrato.

9.2 La parte que adhiere tendrá los mismos derechos y obligaciones que las partes originarias, según la posición asumida de Exportador o Importador y según la categoría correspondiente de agente de tratamiento.

CLAUSE 10. General obligations of the Parties

10.1. The Parties undertake to adopt and, when necessary, demonstrate the implementation of effective measures capable of demonstrating observance of and compliance with the provisions of these Clauses and the National Legislation, as well as with the effectiveness of such measures and, in particular:

a) use the Personal Data only for the specific purposes described in CLAUSE 2, with no possibility of subsequent processing incompatible with such purposes, subject to the limitations, guarantees and safeguards provided for in these Clauses;
b) guarantee the compatibility of the processing with the purposes informed to the Data Subject, according to the processing activity context;

CLÁUSULA 10. Obligaciones generales de las Partes

10.1. Las Partes se comprometen a adoptar y, cuando sea necesario, demostrar la aplicación de medidas eficaces capaces de demostrar la observancia y el cumplimiento de lo dispuesto en estas Cláusulas y la Legislación Nacional, así como la eficacia de dichas medidas y, en particular:

a) utilizar los Datos Personales únicamente para las finalidades específicas descritas en la CLÁUSULA 2, sin posibilidad de tratamiento ulterior incompatible con dichas finalidades, sujeto a las limitaciones, garantías y medidas de protección previstas en estas Cláusulas;
b) garantizar la compatibilidad del tratamiento con las finalidades informadas al Titular de los Datos, según el contexto de la actividad de tratamiento;

c) limit the processing activity to the minimum required for the accomplishment of its purposes, encompassing pertinent, proportional and non- excessive data in relation to the Personal Data processing purposes;
d) guarantee to the Data Subjects, subject to the provisions of Clause 4: (d.1.) clear, accurate and easily accessible information on the processing activities and the respective processing agents, with due regard for trade and industrial secrecy; (d.2.) facilitated and free of charge consultation on the form and duration of the processing, as well as on the integrity of their Personal Data; and (d.3.) accuracy, clarity, relevance and updating of the Personal Data, according to the necessity and for compliance with the purpose of their processing;
e) adopt the appropriate security measures compatible with the risks involved in the International Data Transfer governed by these Clauses;
f) not to process Personal Data for abusive or unlawful discriminatory purposes;
g) ensure that any person acting under their authority, including sub- processors or any agent who collaborates with them, whether for reward or free of charge, only processes data in compliance with their instructions and with the provisions of these Clauses;
h) keep a record of the Personal Data processing operations of the International Data Transfer governed by these Clauses, and submit the relevant documentation to ANPD, when requested.

CLAUSE 11. Sensitive personal data

11.1. If the International Data Transfer involves Sensitive Personal Data, the Parties shall apply additional safeguards, including specific Security Measures which are proportional to the risks of the processing activity, to the specific nature of the data and to the interests, rights and guarantees to be protected, as described in SECTION III.

c) limitar la actividad de tratamiento al mínimo necesario para el cumplimiento de sus finalidades, abarcando datos pertinentes, proporcionales y no excesivos en relación con los fines del tratamiento de los Datos Personales;
d) garantizar a los Titulares de los Datos, sujeto a lo dispuesto en la Cláusula 4: (d.1.) información clara, precisa y de fácil acceso sobre las actividades de tratamiento y los respectivos agentes de tratamiento, con el debido respeto al secreto comercial e industrial; (d.2.) consulta facilitada y gratuita sobre la forma y duración del tratamiento, así como sobre la integridad de sus Datos Personales; y (d.3.) exactitud, claridad, pertinencia y actualización de los Datos Personales, según la necesidad y para el cumplimiento de la finalidad de su tratamiento;
e) adoptar las medidas de seguridad adecuadas compatibles con los riesgos que conlleva la Transferencia Internacional de Datos regida por estas Cláusulas;
f) no tratar Datos Personales con fines discriminatorios abusivos o ilícitos;
g) garantizar que cualquier persona que actúe bajo su autoridad, incluidos los subencargados del tratamiento o cualquier agente que colabore con ellos, ya sea a cambio de una remuneración o de forma gratuita, solamente procese los datos de conformidad con sus instrucciones y con las disposiciones de estas Cláusulas.
h) llevar un registro de las operaciones de tratamiento de Datos Personales de la Transferencia Internacional de Datos regidas por estas Cláusulas, y presentar la documentación pertinente a la ANPD, cuando ésta lo solicite.

CLÁUSULA 11. Datos personales sensibles

11.1. Si la Transferencia Internacional de Datos involucra Datos Personales Sensibles, las Partes aplicarán medidas de protección adicionales, incluyendo Medidas de Seguridad específicas que sean proporcionales a los riesgos de la actividad de tratamiento, a la naturaleza específica de los datos y a

los intereses, derechos y garantías que se protejan, tal y como se describe en la SECCIÓN III.

CLAUSE 12. Personal data of children and adolescents

12.1. In case the International Data Transfer governed by these Clauses involves Personal Data concerning children and adolescents, the Parties shall implement measures to ensure that the processing is carried out in their best interest, under the terms of the National Legislation and relevant instruments of international law.

CLÁUSULA 12. Datos personales de niños, niñas y adolescentes

12.1. En caso de que la Transferencia Internacional de Datos regida por estas Cláusulas involucre Datos Personales relativos a niños, niñas y adolescentes, las Partes implementarán medidas para garantizar que el tratamiento se realice en su mejor interés, en los términos de la Legislación Nacional y los instrumentos de derecho internacional pertinentes.

CLAUSE 13. Legal use of data

13.1. The Exporter guarantees that Personal Data has been collected, processed and transferred to the Importer in accordance with the National Legislation.

CLÁUSULA 13. Uso legítimo de datos

13.1. El Exportador garantiza que los Datos Personales han sido recopilados, procesados y transferidos al Importador de conformidad con la Legislación Nacional

CLAUSE 14. Transparency

14.1. The Designated Party shall publish, on its website, a document containing easily accessible information written in simple, clear and accurate language on the conduction of the International Data Transfer, including at least information on:

a) the form, duration and specific purpose of the international transfer;
b) the destination country of the transferred data;
c) the Designated Party's identification and contact details;
d) the shared use of data by the Parties and its purpose;
e) the responsibilities of the agents who shall conduct the processing;
f) the Data Subject's rights and the means for exercising them, including an easily accessible channel made available to respond to their requests, and the right to file a petition against the Exporter and the Importer before ANPD; and
g) Onward Transfers, including those relating to recipients and to the purpose of such transfer.

CLÁUSULA 14. Transparencia

14.1. La Parte Designada deberá publicar, en su sitio web, un documento que contenga información de fácil acceso redactada en un lenguaje sencillo, claro y preciso sobre la realización de la Transferencia Internacional de Datos, incluyendo al menos información sobre

a) la forma, duración y finalidad específica de la transferencia internacional;
b) el país de destino de los datos transferidos;
c) la identificación y los datos de contacto de la Parte Designada;
d) el uso compartido de los datos por las Partes y su finalidad;
e) las responsabilidades de los agentes que realizarán el tratamiento;
f) los derechos del Titular de los Datos y los medios para ejercerlos, incluyendo un canal de fácil acceso para responder a sus solicitudes, y el derecho a presentar una demanda contra el Exportador y el Importador ante la ANPD; y
g) Transferencias Posteriores, incluyendo las relativas a los destinatarios y a la finalidad de dicha transferencia.

14.2. The document referred to in item 14.1. shall be made available on a specific website page

14.2. El documento al que se refiere el punto 14.1. deberá estar disponible en una página web específica o

or integrated, in a prominent and easily accessible format, to the Privacy Policy or equivalent document.

14.3. Upon request, the Parties shall make a copy of these Clauses available to the Data Subject free of charge, complying with trade and industrial secrecy.

14.4. All information made available to Data Subjects, under the terms of these Clauses, shall be written in Portuguese.

CLAUSE 15. Rights of the data subject

15.1. The Data subject shall have the right to obtain from the Designated Party, as regards the Personal Data subject to the International Data Transfer governed by these Clauses, at any time, and upon request, under the terms of the National Legislation:

a) confirmation of the existence of processing;
b) access to data;
c) correction of incomplete, inaccurate or outdated data;
d) anonymization, blocking or erasure of unnecessary or excessive data or data processed in noncompliance with these Clauses and the provisions of National Legislation;
e) portability of data to another service or product provider, upon express request, in accordance with ANPD regulations, complying with trade and industrial secrecy;
f) erasure of Personal Data processed under the Data Subject's consent, except for the events provided in CLAUSE 20;
g) information on public and private entities with which the Parties have shared data;
h) information on the possibility of denying consent and on the consequences of the denial;
i) withdrawal of consent through a free of charge and facilitated procedure, remaining ratified the processing activities carried out before the request for elimination;

integrado, en un formato destacado y de fácil acceso, en la Política de Privacidad o documento equivalente.

14.3. Las Partes pondrán a disposición del Titular de los Datos, previa solicitud, una copia de estas Cláusulas de forma gratuita, cumpliendo con el secreto comercial e industrial.

14.4. Toda la información puesta a disposición de los Titulares de los Datos, en los términos de estas Cláusulas, deberá estar redactada en portugués.

CLÁUSULA 15. Derechos del titular de datos

15.1. El Titular de los Datos tendrá derecho a obtener de la Parte Designada, respecto de los Datos Personales objeto de la Transferencia Internacional de Datos regida por estas Cláusulas, en cualquier momento, y previa solicitud, en los términos de la Legislación Nacional:

a) confirmación de la existencia del tratamiento;
b) acceso a los datos;
c) corrección de datos incompletos, inexactos u obsoletos;
d) anonimización, bloqueo o supresión de datos innecesarios o excesivos, o de datos tratados en incumplimiento de estas Cláusulas y de las disposiciones de la legislación nacional;
e) portabilidad de los datos a otro proveedor de servicios o productos, previa solicitud expresa, de conformidad con las disposiciones de la ANPD y en cumplimiento del secreto comercial e industrial;
f) supresión de los Datos Personales tratados con el consentimiento del Titular, salvo en los supuestos previstos en la CLÁUSULA 20;
g) información sobre las entidades públicas y privadas con las que las Partes han compartido datos;
h) información sobre la posibilidad de denegar el consentimiento y las consecuencias de dicha denegación;
i) revocación del consentimiento mediante un procedimiento gratuito y simplificado, quedando ratificadas las actividades de tratamiento realizadas antes de la solicitud de supresión;
j) revisión de decisiones adoptadas únicamente sobre la base del

j) review of decisions taken solely on the basis of automated processing of personal data affecting their interests, including decisions aimed at defining their personal, professional, consumer and credit profile or aspects of their personality; and
k) information on the criteria and procedures adopted for the automated decision.

15.2. Data subject may oppose to the processing based on one of the events of waiver of consent, in case of noncompliance with the provisions of these Clauses or National Legislation.

15.3. The deadline for responding to the requests provided for in this Clause and in item 14.3 is 15 (fifteen) days from the date of the data subject's request, except in the event of a different deadline established in specific ANPD regulations.

15.4. In case the Data Subject's request is directed to the Party not designated as responsible for the obligations set forth in this Clause or in item 14.3., the referred Party shall:

a) inform the Data Subject of the service channel made available by the Designated Party; or
b) forward the request to the Designated Party as early as possible, to enable the response within the period provided in item 15.2.

15.5. The Parties shall immediately inform the Data Processing Agents with whom they have shared data with the correction, deletion, anonymization or blocking of the data, for them to follow the same procedure, except in cases where this communication is demonstrably impossible or involves a disproportionate effort.

15.6. The Parties shall promote mutual assistance to respond to the Data Subjects' requests.

CLAUSE 16. Security Incident Reporting

16.1. The Designated Party shall notify ANPD and the Data Subject, within 3 (three) working days of the occurrence of a security incident that may entail a relevant risk or damage to the Data

tratamiento automatizado de datos personales que afecten a sus intereses, incluidas las decisiones dirigidas a definir su perfil personal, profesional, de consumo y crediticio o aspectos de su personalidad; y
k) información sobre los criterios y procedimientos adoptados para la decisión automatizada.

15.2. El titular de los datos podrá oponerse al tratamiento con base en alguno de los supuestos de renuncia del consentimiento, en caso de incumplimiento de lo dispuesto en estas Cláusulas o en la Legislación Nacional.

15.3. El plazo para responder a las solicitudes previstas en esta Cláusula y en el punto 14.3 es de 15 (quince) días contados desde la fecha de la solicitud del titular de los datos, salvo que se haya establecido un plazo distinto establecido en la normativa específica de la ANPD.

15.4. En caso de que la solicitud del Titular de los Datos se dirija a la Parte no designada como responsable de las obligaciones previstas en la presente Cláusula o en el punto 14.3., la Parte referida deberá:

a) informar al Titular de los Datos sobre el canal de atención puesto a disposición por la Parte Designada; o
b) remitir la solicitud a la Parte Designada lo antes posible, a fin de posibilitar la respuesta dentro del plazo previsto en el punto 15.2.

15.5. Las Partes deberán informar inmediatamente a los Encargados del Tratamiento de Datos con quienes hayan compartido datos sobre la corrección, supresión, anonimización o bloqueo de los mismos, para que sigan el mismo procedimiento, salvo en los casos en que esta comunicación sea manifiestamente imposible o suponga un esfuerzo desproporcionado.

15.6. Las Partes promoverán la asistencia mutua para responder a las solicitudes de los Titulares de los Datos

CLÁUSULA 16. Denuncia de Incidente de Seguridad

16.1. La Parte Designada deberá notificar a la ANPD y al Titular de los Datos, dentro de los 3 (tres) días hábiles siguientes a la ocurrencia de un incidente de

Subjects, according to the provisions of National Legislation.

16.2. The Importer must keep a record of security incidents in accordance with National Legislation.

CLAUSE 17. Liability and compensation for damages

17.1. The Party which, when performing Personal Data processing activities, causes patrimonial, moral, individual or collective damage, for violating the provisions of these Clauses and of the National Legislation, shall compensate for it.

17.2. Data Subject may claim compensation for damage caused by any of the Parties as a result of a breach of these Clauses.

17.3. The defense of Data Subjects' interests and rights may be claimed in court, individually or collectively, in accordance with the provisions in relevant legislation regarding the instruments of individual and collective protection.

17.4. The Party acting as Processor shall be jointly and severally liable for damages caused by the processing activities when it fails to comply with these Clauses or when it has not followed the lawful instructions of the Controller, except for the provisions of item 17.6.

17.5. The Controllers directly involved in the processing activities which resulted in damage to the Data Subject shall be jointly and severally liable for these damages, except for the provisions of item 17.6.

17.6. Parties shall not be held liable if they have proven that:

a) they have not carried out the processing of Personal Data attributed to them;
b) although they did carry out the processing of Personal Data attributed to them, there was no violation of these Clauses or National Legislation; or
c) the damage results from the sole fault of the Data Subject or of a third- party which

seguridad que pueda implicar un riesgo o daño relevante para los Titulares de los Datos, de acuerdo con lo dispuesto en la Legislación Nacional.

16.2. El Importador deberá mantener un registro de los incidentes de seguridad de acuerdo con la Legislación Nacional

CLÁUSULA 17. Responsabilidad e indemnización por daños y perjuicios

17.1. La Parte que, al realizar actividades de Tratamiento de Datos Personales, cause daños y perjuicios patrimoniales, morales, individuales o colectivos, por incumplir lo dispuesto en estas Cláusulas y en la Legislación Nacional, deberá indemnizar por ellos.

17.2. El Titular de los Datos podrá reclamar la indemnización por los daños y perjuicios que le ocasione cualquiera de las Partes como consecuencia del incumplimiento de estas Cláusulas.

17.3. La defensa de los intereses y derechos de los Titulares de los Datos podrá reclamarse en sede judicial, de forma individual o colectiva, de conformidad con lo dispuesto en la legislación aplicable relativa a los instrumentos de protección individual y colectiva.

17.4. La Parte que actúe como Encargado del Tratamiento será solidariamente responsable de los daños y perjuicios causados por las actividades de tratamiento cuando no cumpla con estas Cláusulas o cuando no haya seguido las instrucciones lícitas del Responsable, con excepción de lo dispuesto en el punto 17.6.

17.5. Los Responsables directamente implicados en las actividades de tratamiento que hayan producido daños al Titular de los Datos serán solidariamente responsables de dichos daños, con excepción de lo dispuesto en el punto 17.6.

17.6. Las partes no serán responsables si han probado que:

a) no han llevado a cabo el tratamiento de los Datos Personales que se les atribuye;
b) si bien llevaron a cabo el tratamiento de los Datos Personales que se les atribuye, no se ha infringido ninguna de las presentes Cláusulas ni la Legislación Nacional; o

is not a recipient of the Onward Transfer or not subcontracted by the Parties.

17.7. Under the terms of the National Legislation, the judge may reverse the burden of proof in favor of the Data Subject whenever, in his judgement, the allegation is credible, there is a lack of sufficient evidence or when the Data Subject would be excessively burdened by the production of evidence.

17.8. Judicial proceedings for compensation for collective damages which intend to establish liability under the terms of this Clause may be collectively conducted in court, with due regard for the provisions in relevant legislation.

17.9. The Party which compensates the damage to the Data Subject shall have a right of recourse against the other responsible parties, to the extent of their participation in the damaging event.

CLAUSE 18. Safeguards for Onward Transfers

The Importer shall only carry out Onward Transfers of Personal Data subject to the International Data Transfer governed by these Clauses if expressly authorized, in accordance with the terms and conditions described in CLAUSE 3.

18.1. In any case, the Importer:

a) shall ensure that the purpose of the Onward Transfer is compatible with the specific purposes described in CLAUSE 2;
b) shall guarantee, by means of a written contractual instrument, that the safeguards provided in these Clauses shall be ensured by the third-party recipient of the Onward Transfer; and
c) for the purposes of these Clauses, and regarding the Personal Data transferred, shall be considered responsible for any eventual irregularities committed by the third-party recipient of the Onward Transfer.

18.2. The Onward Transfer shall also be carried out based on another valid modality of International Data Transfer provided in National Legislation, regardless of the authorization referred to in CLAUSE 3.

c) el daño sea consecuencia exclusiva de la responsabilidad del Titular de los Datos o de un tercero que no sea destinatario de la Transferencia Posterior ni subcontratado por las Partes.

17.7. En los términos de la Legislación Nacional, el juez podrá invertir la carga de la prueba a favor del Titular de los Datos cuando, a su criterio, la acusación sea creíble, exista falta de prueba suficiente o cuando el Titular de los Datos resulte excesivamente cargado con la presentación de la prueba.

17.8. Los procedimientos judiciales de indemnización por daños y perjuicios colectivos que tengan por objeto establecer la responsabilidad en los términos de esta Cláusula podrán sustanciarse de forma colectiva ante los tribunales, con el debido respeto a lo dispuesto en la legislación aplicable.

17.9. La Parte que indemnice por los daños y perjuicios causados al Titular de los Datos tendrá derecho a repetir contra los demás responsables, en la medida de su participación en el hecho causante de los daños y perjuicios.

CLÁUSULA 18. Medidas de protección para las Transferencias Posteriores

El Importador sólo podrá realizar Transferencias Posteriores de Datos Personales sujetas a la Transferencia Internacional de Datos regida por estas Cláusulas si así se lo autoriza expresamente, de conformidad con los términos y condiciones descritos en la CLÁUSULA 3.

18.1. En cualquier caso, el Importador deberá:

a) garantizar que la finalidad de la Transferencia Posterior sea compatible con las finalidades específicas descritas en la CLÁUSULA 2;
b) garantizar, mediante un instrumento contractual escrito, que el tercero destinatario de la Transferencia Posterior asegure las medidas de protección previstas en estas Cláusulas; y
c) a los efectos de estas Cláusulas, y en relación con los Datos Personales transferidos, será considerado responsable de cualquier irregularidad cometida por el tercero destinatario de la Transferencia Posterior.

18.2. La Transferencia Posterior también deberá realizarse con base en otra modalidad vigente de Transferencia Internacional de Datos prevista en la

CLAUSE 19. Access Request Notification

19.1 The Importer shall notify the Exporter and the Data Subject of any Access Request related to the Personal Data subject to the International Data Transfer governed by these Clauses, except in the event that notification is prohibited by the law of the country in which the data is processed.

19.2. The Importer shall implement the appropriate legal measures, including legal actions, to protect the rights of the Data Subjects whenever there is adequate legal basis to question the legality of the Access Request and, if applicable, the prohibition of issuing the notification referred to in item 19.1.

19.3. To comply with both the ANPD's and the Exporter's requests, the Importer shall keep a record of Access Requests, including date, requester, purpose of the request, type of data requested, number of requests received, and legal measures implemented.

CLAUSE 20. Termination of processing and erasure of data

20.1. Parties shall erase the personal data subject to the International Data Transfer governed by these Clauses after the ending of their processing, being their storage authorized only for the following purposes:

a) compliance with a legal or regulatory obligation by the Controller;
b) study by a Research Body, guaranteeing, whenever possible, the anonymization of personal data;
c) transfer to a third-party, upon compliance with requirements set forth in these Clauses and in the National Legislation; and
d) exclusive use of the Controller, being the access by a third-party prohibited, and provided data have been anonymized.

20.2. For the purposes of this Clause, processing of personal data shall cease when:

Legislación Nacional, independientemente de la autorización a que se refiere la CLÁUSULA 3.

CLÁUSULA 19. Notificación de Solicitud de Acceso

19.1 El Importador deberá notificar al Exportador y al Titular de los Datos cualquier Solicitud de Acceso relacionada con los Datos Personales objeto de la Transferencia Internacional de Datos regida por estas Cláusulas, salvo en caso de que la notificación esté prohibida por la ley del país en el que se procesen los datos.

19.2. El Importador deberá implementar las medidas legales apropiadas, incluyendo acciones judiciales, para proteger los derechos de los Titulares de los Datos siempre que exista base legal adecuada para cuestionar la legalidad de la Solicitud de Acceso y, en su caso, la prohibición de emitir la notificación a que se refiere el punto 19.1.

19.3. Para cumplir con las solicitudes de la ANPD y del Exportador, el Importador deberá mantener un registro de las Solicitudes de Acceso, incluyendo fecha, solicitante, propósito de la solicitud, tipo de datos solicitados, número de solicitudes recibidas y medidas legales implementadas.

CLÁUSULA 20. Terminación del tratamiento y supresión de datos

20.1. Las Partes deberán suprimir los datos personales objeto de la Transferencia Internacional de Datos regida por estas Cláusulas una vez finalizado su tratamiento, y su almacenamiento estará autorizado únicamente para las siguientes finalidades:

a) cumplimiento de una obligación legal o reglamentaria por parte del Responsable;
b) estudio por parte de un Organismo de Investigación, garantizando, siempre que sea posible, la anonimización de los datos personales;
c) transferencia a un tercero, previo cumplimiento de los requisitos establecidos en estas Cláusulas y en la Legislación Nacional; y
d) uso exclusivo del Responsable, quedando prohibido el acceso a terceros, siempre que los datos hayan sido anonimizados.

20.2. A los efectos de la presente Cláusula, el tratamiento de los datos personales cesará cuando:

a) the purpose set forth in these Clauses has been achieved;
b) Personal Data are no longer necessary or pertinent to attain the intended specific purpose set forth in these Clauses;
c) at the termination of the treatment period;
d) Data Subject's request is met; and
e) at the order of ANPD, upon violation of the provisions of these Clauses or National Legislation.

a) Se haya cumplido la finalidad establecida en estas Cláusulas;
b) Los Datos Personales ya no sean necesarios o pertinentes para alcanzar la finalidad específica prevista en estas Cláusulas;
c) Al finalizar el periodo de tratamiento;
d) Se haya satisfecho la solicitud del Titular de los Datos; y
e) Por orden de la ANPD, en caso de incumplimiento de lo dispuesto en estas Cláusulas o en la legislación nacional.

CLAUSE 21. Data processing security

21.1. Parties shall implement Security Measures which guarantee sufficient protection of the Personal Data subject to the International Data Transfer governed by these Clauses, even after its termination.

21.2. Parties shall inform, in SECTION III, the Security Measures implemented, considering the nature of the processed information, the specific characteristics and the purpose of the processing, the technology current state and the probability and severity of the risks to the Data Subjects' rights, especially in the case of sensitive personal data and that of children and adolescents.

21.3. The Parties shall make the necessary efforts to implement periodic evaluation and review measures to maintain the appropriate level of data security.

CLÁUSULA 21. Seguridad de tratamiento de datos

21.1. Las Partes deberán implementar Medidas de protección que garanticen la protección suficiente de los Datos Personales objeto de la Transferencia Internacional de Datos regulada por estas Cláusulas, incluso después de su terminación.

21.2. Las Partes deberán informar, en la SECCIÓN III, las Medidas de Seguridad implementadas, considerando la naturaleza de la información tratada, las características específicas y la finalidad del tratamiento, el estado actual de la tecnología y la probabilidad y gravedad de los riesgos para los derechos de los Titulares de los Datos Personales, especialmente cuando se trate de datos personales sensibles y de niños, niñas y adolescentes.

21.3. Las Partes realizarán los esfuerzos necesarios para implementar medidas de evaluación y revisión periódicas para mantener el nivel adecuado de seguridad de los datos.

CLAUSE 22. Legislation of country of destination

22.1 The Importer declares that it has not identified any laws or administrative practices of the country receiving the Personal Data that prevent it from fulfilling the obligations assumed in these Clauses.

22.2. In the event of a regulatory change which alters this situation, the Importer shall immediately notify the Exporter to assess the continuity of the contract.

CLÁUSULA 22. Legislación del país de destino

22.1 El Importador declara que no ha identificado leyes o prácticas administrativas del país receptor de los Datos Personales que le impidan cumplir con las obligaciones asumidas en estas Cláusulas.

22.2. En caso de cambio normativo que altere esta situación, el Importador deberá notificarlo inmediatamente al Exportador para evaluar la continuidad del contrato.

CLAUSE 23. Non-compliance with the Clauses by the Importer

CLÁUSULA 23. Incumplimiento de las cláusulas por parte del Importador

23.1. In the event of a breach in the safeguards and guarantees provided in these Clauses or being the Importer unable to comply with any of them, the Exporter shall be immediately notified, subject to the provisions in item 19.1.

23.2. Upon receiving the communication referred to in item 23.1 or upon verification of non-compliance with these Clauses by the Importer, the Exporter shall implement the relevant measures to ensure the protection of the Data Subjects' rights and the compliance of the International Data Transfer with the National Legislation and these Clauses, and may, as appropriate:

a) suspend the International Data Transfer;
b) request the return of the Personal Data, its transfer to a third-party, or its erasure; and
c) terminate the contract.

CLAUSE 24. Choice of forum and jurisdiction

24.1. Brazilian legislation applies to these Clauses and any controversy between the Parties arising from these Clauses shall be resolved before the competent courts in Brazil, observing, if applicable, the forum chosen by the Parties in Section IV.

24.2. Data Subjects may file lawsuits against the Exporter or the Importer, as they choose, before the competent courts in Brazil, including those in their place of residence.

24.3. By mutual agreement, Parties may use arbitration to resolve conflicts arising from these Clauses, provided that the procedure is carried out in Brazil and in accordance with the provisions of the Arbitration Law.

SECTION III - Security Measures

(NOTE: This Section should include details of the security measures implemented, including specific measures for the protection of sensitive data and children and adolescents. The measures may include the following aspects, among others, as indicated in the table below).

(i) governance and supervision of internal processes:
(ii) technical and administrative security measures, including measures to

23.1. En caso de incumplimiento de las medidas de protección y garantías previstas en estas Cláusulas o de no poder cumplir el Importador con alguna de ellas, deberá notificarse inmediatamente al Exportador, sujeto a lo dispuesto en el punto 19.1.

23.2. Al recibir la comunicación a que se refiere el punto 23.1 o al verificarse el incumplimiento de estas Cláusulas por parte del Importador, el Exportador deberá implementar las medidas pertinentes para asegurar la protección de los derechos de los Titulares de los Datos y la conformidad de la Transferencia Internacional de Datos con la Legislación Nacional y estas Cláusulas, y podrá, según corresponda:

a) suspender la Transferencia Internacional de Datos;
b) solicitar la devolución de los Datos Personales, su transferencia a un tercero o su supresión; y
c) rescindir el contrato.

CLÁUSULA 24. Elección de fuero y jurisdicción

24.1. La legislación brasileña se aplica a estas Cláusulas y cualquier controversia entre las Partes que surja de estas Cláusulas se resolverá ante los tribunales competentes en Brasil, y se observará, si corresponde, el fuero elegido por las Partes en la Sección IV.

24.2. Los titulares de los datos podrán presentar acciones judiciales contra el Exportador o el Importador, según su elección, ante los tribunales competentes en Brasil, incluyendo los de su lugar de residencia.

24.3. De común acuerdo, las Partes podrán recurrir al arbitraje para resolver los conflictos derivados de estas Cláusulas, siempre que el procedimiento se lleve a cabo en Brasil y de conformidad con las disposiciones de la Ley de Arbitraje.

SECCIÓN III – Medidas de Seguridad

(NOTA: Esta sección debe incluir detalles de las medidas de seguridad implementadas, incluyendo medidas específicas para la protección de datos sensibles y datos de niños, niñas y adolescentes. Las medidas pueden incluir, entre otros, los siguientes aspectos, como se indica en la tabla a continuación.).

(i) gobernanza y supervisión de los procesos internos;
(ii) medidas de seguridad técnicas y administrativas, incluidas las medidas para

guarantee the security of the operations carried out, such as the collection, transmission and storage of data:

garantizar la seguridad de las operaciones realizadas, como la recopilación, transmisión y almacenamiento de datos:

SECTION IV - Additional Clauses and Annexes

(NOTE: In this Section, which is optional to complete and to disclose, Additional Clauses and Annexes may be included, at the discretion of the Parties, to regulate, among other things, issues of a commercial nature, contractual termination, term of validity and choice of forum in Brazil. As provided for in the International Data Transfer Regulation, the clauses established in this Section or in Related Contracts may not exclude, modify or contradict, directly or indirectly, the Clauses provided in Sections I, II and III).

SECCIÓN IV – Cláusulas y Anexos Adicionales

(NOTA: En esta Sección, cuya cumplimentación y divulgación son opcionales, se podrán incluir, a discreción de las Partes, Cláusulas Adicionales y Anexos para regir, entre otras cosas, cuestiones de carácter comercial, la extinción del contrato, el plazo de validez y la elección de fuero en Brasil. Según lo dispuesto en el Reglamento de Transferencia Internacional de Datos, las cláusulas establecidas en esta Sección o en los Contratos Relacionados no podrán excluir, modificar ni contradecir, directa o indirectamente, las cláusulas previstas en las Secciones I, II y III.).