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

ADENDO SOBRE TRATAMENTO DE DADOS
("DPA") PARA A CHS INC. FORNECEDORES
CONTROLADOR PARA OPERADOR (C2P)

A fim de cumprir suas obrigações nos termos dos regulamentos aplicáveis de proteção e segurança de dados, a CHS Inc. e suas Afiliadas (doravante denominadas "CHS") compartilharão determinados Dados Pessoais com [Insira o nome do prestador de serviços/fornecedor] (doravante denominado "Fornecedor") sujeitos aos termos deste adendo (doravante denominado "Adendo") e somente na medida do necessário para que o Fornecedor cumpra suas obrigações nos termos do [Insira o nome do contrato de prestação de serviços] (doravante denominado "Contrato Principal"). O Fornecedor atuará como um "agente" da CHS para os fins limitados de uso, armazenamento e tratamento desses Dados Pessoais. Este Adendo pode ser assinado em uma ou mais vias, cada uma das quais será considerada um original, mas todas juntas constituirão um único e mesmo contrato.

1. **Definições.** Para os fins do presente Adendo, os termos a seguir terão os seguintes significados.

   a. **Afiliada(s)**: significa qualquer outra pessoa jurídica que, direta ou indiretamente, através de um ou mais intermediários, controle, seja controlada por ou esteja sob controle comum com tal entidade. O termo "controlar" (incluindo os termos "controlada por" e "sob controle comum com") significa o poder direto ou indireto de dirigir ou causar a direção da gestão e das políticas de uma entidade, seja através da propriedade de títulos com direito a voto, por contrato ou de outra forma, de mais de cinquenta por cento (50%) dos títulos com direito a voto de uma entidade.
   b. **"Leis de Privacidade de Dados"** significa quaisquer leis que se apliquem ao Tratamento de Dados Pessoais pelo Fornecedor nos termos do Contrato Principal. Isso inclui leis, regulamentos, diretrizes, requisitos e regras emitidas pelo governo nos EUA e em outras jurisdições, em nível internacional, nacional, estadual/provincial ou local, atualmente em vigor e à medida que entrarem em vigor, incluindo, sem limitação, a Diretiva

(Regulation (EU) 2016/679) ("GDPR"), the UK Data Protection Act, 2018, the California 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.

95/46/CE da UE, o Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) 2016/679) ("RGPD"), a Lei de Proteção de Dados do Reino Unido, 2018, a Lei de Privacidade do Consumidor da Califórnia de 2018 ("CCPA"), conforme alterada pela Lei de Direitos de Privacidade da Califórnia de 2020 ("CPRA"), a Lei de Proteção de Dados do Consumidor da Virgínia ("VCDPA"), a Lei de Privacidade do Colorado ("CPA"), a Lei SHIELD de Nova York, a Lei Federal para a Proteção de Dados Pessoais detidos por Partes Privadas e seus regulamentos ("FDPL"), a Lei de Proteção de Dados do Brasil nº 13.709/2018 (a "LGPD") e quaisquer leis de segurança e/ou privacidade de dados aplicáveis de outras jurisdições, conforme possam ser alteradas de tempos em tempos.

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

c. **"Titular dos Dados"** significa a pessoa física a quem os Dados Pessoais se relacionam.

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.

d. **"Sistemas de Informações"** significam equipamentos, sistemas e serviços de informática, comunicação e rede (voz, dados ou outros) de propriedade, controle ou uso da CHS, incluindo, entre outros, a rede de área ampla corporativa, a rede comutada, gateways de inter/intranet, correio eletrônico, telefonia, sistemas de informática, hardware do sistema, drives, mídia eletrônica, áreas de armazenamento, programas de software, arquivos e bancos de dados.

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.

e. **"Sistema Permitido"** significa um Sistema de Informações da CHS a que a CHS ou Afiliadas da CHS dão expressamente acesso ao Fornecedor e que é necessário para que o Fornecedor cumpra suas obrigações perante a 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.

f. **"Dados Pessoais"** significa qualquer informação recebida pelo Fornecedor da CHS, ou em nome da CHS, que identifique, se relacione, descreva, seja razoavelmente capaz de ser associada ou possa ser razoavelmente vinculada, direta ou indiretamente, a um indivíduo ou família específica.

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.

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.

g. **"Tratar" ou "Tratamento"** significa qualquer operação ou conjunto de operações realizadas sobre Dados Pessoais, por meios automatizados ou não, tais como coleta, registro, organização, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, bloqueio, apagamento ou destruição.

h. **"Incidente de Segurança"** significa qualquer acesso ilegal ou não autorizado a quaisquer Dados Pessoais da CHS armazenados no equipamento ou nas instalações do Fornecedor, ou acesso a equipamentos ou instalações que resulte em qualquer uso, aquisição, tratamento, perda, destruição, dano, divulgação, roubo, cópia, modificação ou alteração não autorizados dos Dados Pessoais da CHS.

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

2. Obrigações do Fornecedor.

O Fornecedor declara e garante que:

a. Tratará os Dados Pessoais em nome da CHS, apenas para cumprir as suas obrigações nos termos do(s) Contrato(s) Principal(is) ou conforme instruído por escrito pela CHS, e em conformidade com todas as Leis de Privacidade de Dados aplicáveis e os termos deste Adendo, e abster-se-á de tratar Dados Pessoais para fins diferentes dos instruídos pela CHS. Além disso, o Fornecedor deve manter a confidencialidade dos Dados Pessoais que estão sendo tratados. Para evitar dúvidas, o Fornecedor está proibido de: (i) vender, alugar, divulgar, disseminar, disponibilizar, transferir ou comunicar de outra forma, oralmente ou por escrito, ou por meios eletrônicos ou outros, os Dados Pessoais a outra entidade (seja ela afiliada ou não) (iii) reter, usar ou divulgar os Dados Pessoais fora do relacionamento entre a CHS e o Fornecedor; e (iv) combinar os Dados Pessoais com quaisquer outros dados pessoais tratados pelo Fornecedor fora de seu relacionamento com a CHS, exceto

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 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

conforme expressamente permitido pelo Contrato Principal.

b. Notificará a CHS por escrito, incluindo um aviso para privacy@chsinc.com, imediatamente após determinar que não cumpriu ou não pode mais cumprir suas obrigações nos termos da Cláusula 2, alínea a) deste Adendo. Nesse caso, o Fornecedor cumprirá as instruções escritas da CHS, incluindo instruções para cessar o tratamento dos Dados Pessoais, e tomará todas as medidas necessárias para remediar qualquer tratamento desses Dados Pessoais que não esteja em conformidade com a Cláusula 2, alínea a) deste Adendo.

c. Apresentará as suas instalações de tratamento de dados, ficheiros de dados e documentação necessária para o Tratamento dos Dados Pessoais para auditoria e/ou revisão pela CHS ou por qualquer auditor independente ou entidade de inspeção razoavelmente selecionada pela CHS para verificar o cumprimento do presente Adendo, mediante pedido da CHS, com aviso prévio razoável e durante o horário normal de expediente. Quaisquer dados e documentação divulgados no decorrer de tal auditoria serão mantidos em sigilo para fins de obrigação de confidencialidade, se houver, nos termos de qualquer Contrato Principal entre o Fornecedor e a CHS.

d. Obterá a aprovação prévia por escrito da CHS, que inclui aviso por e-mail para privacy@chsinc.com, para divulgar Dados Pessoais a terceiros ou permitir que terceiros acessem Dados Pessoais; e, nesse caso, deverá: (i) celebrar um contrato por escrito com o suboperador terceiro que imponha obrigações substancialmente semelhantes às estabelecidas neste Adendo, conforme exigido pelas Leis de Privacidade de Dados aplicáveis; (ii)

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 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.

impor os mesmos requisitos de privacidade e segurança a qualquer terceiro ao qual o Fornecedor esteja sujeito nos termos deste Adendo; (iii) permanecer responsável por quaisquer ações de terceiros em relação aos Dados Pessoais; e (iv) fornecer à CHS, pelo menos 30 dias antes de divulgar ou permitir o acesso a quaisquer Dados Pessoais, uma lista detalhando o nome e endereço de todos os terceiros aos quais divulga ou permite o acesso a Dados Pessoais, incluindo os locais dos servidores desses terceiros que hospedam ou tratam Dados Pessoais, a fim de permitir que a CHS avalie se são necessários acordos suplementares de tratamento de dados ou outros controles para proteger os Dados Pessoais e/ou decidir se recusa a aprovação da subcontratação a quaisquer desses terceiros. O Fornecedor também deverá notificar a CHS por escrito sobre quaisquer alterações pretendidas relativas à adição ou substituição de suboperadores terceirizados, proporcionando assim à CHS a oportunidade de se opor a tais alterações em tempo hábil. O Fornecedor será responsabilizado por todas e quaisquer ações ou omissões por parte dele ou de seu subcontratado com relação à violação deste Adendo.

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

e. O Fornecedor prestará assistência à CHS conforme possa ser razoavelmente necessário para que a CHS cumpra as leis de proteção de dados aplicáveis, incluindo, mas não se limitando a, (i) auxiliar a CHS na resposta a solicitações de titulares de dados para o exercício dos direitos dos titulares de dados nos termos das Leis de Privacidade de Dados aplicáveis (ii) auxiliar a CHS a responder às solicitações da autoridade de proteção de dados ou outras solicitações reguladoras de informações relacionadas ao Tratamento do Fornecedor; (iii) fornecer todas as informações necessárias relacionadas ao Tratamento do Fornecedor para que a CHS demonstre conformidade com as leis de

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 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

proteção de dados aplicáveis; e (iv) fornecer assistência razoável à CHS quando a CHS estiver conduzindo uma avaliação de impacto de privacidade ou transferência. Especificamente, o Fornecedor concorda que tem a capacidade técnica e deve ajudar a CHS a excluir com segurança os Dados Pessoais, bem como fornecer à CHS uma lista de elementos de Dados Pessoais sobre um indivíduo específico mantido pelo Fornecedor em nome da CHS, mediante solicitação da CHS e no prazo de 15 dias após o recebimento de tal solicitação.

f. Notificar prontamente, mas no prazo máximo de quarenta e oito (48) horas, a CHS se receber um pedido de acesso ao assunto, retificação, cancelamento, objeção, restrição, portabilidade de dados ou revogação de consentimento para o Tratamento de Dados Pessoais, ou quaisquer outros pedidos relacionados com a proteção de dados. O Fornecedor não responderá a tais solicitações diretamente, a menos que expressamente autorizado pela CHS por escrito. Caso qualquer tribunal, agência governamental ou agência de aplicação da lei entre em contato com o Fornecedor com uma demanda pelos Dados da CHS, o Fornecedor orientará a agência de aplicação da lei a solicitar tais informações diretamente à CHS. Como parte desse esforço, o Fornecedor poderá fornecer as informações básicas de contato da CHS para a agência. Se for obrigado a divulgar os Dados da CHS para as autoridades policiais, o Fornecedor deverá notificar a CHS imediatamente, e sem atrasos indevidos, e entregar uma cópia da solicitação (exceto quando o Fornecedor for legalmente proibido de fazê-lo) para permitir que a CHS busque uma ordem de proteção ou qualquer outro recurso apropriado. Na medida do permitido pela lei aplicável, o Fornecedor deverá tomar todas as medidas razoáveis para evitar a divulgação dos Dados Pessoais da CHS a uma agência governamental e/ou em

object, unless prohibited by applicable law.

resposta a uma demanda legal, como intimação ou demanda similar, sem o consentimento prévio e expresso por escrito da CHS. Se e somente na medida em que isso não for legalmente possível, o Fornecedor notificará a CHS com antecedência de qualquer divulgação e dará à CHS a oportunidade de se opor, a menos que seja proibido pela lei aplicável.

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

3. **Programa de Segurança da Informação.** Com relação aos Dados Pessoais transferidos ou recebidos pelo Fornecedor nos termos do(s) Contrato(s) Principal(is), o Fornecedor implementou e manterá um programa abrangente de segurança da informação por escrito ("Programa de Segurança da Informação") que inclui proteções administrativas, técnicas, organizacionais e físicas para garantir a confidencialidade, segurança, integridade e disponibilidade dos Dados Pessoais e para proteger contra acesso não autorizado, uso, divulgação, alteração ou destruição de Dados Pessoais. O Fornecedor deverá avaliar e atualizar regularmente o Programa de Segurança da Informação para refletir novos riscos ou mudanças nas leis e regulamentos aplicáveis, mas não deverá fazer nenhuma mudança que altere ou reduza materialmente as medidas estabelecidas no Programa de Segurança da Informação do Fornecedor. Quando os Dados Pessoais de titulares de dados coreanos estiverem envolvidos, o Programa de Segurança da Informação também deverá incluir as salvaguardas exigidas pela legislação aplicável, incluindo, entre outros, a Lei de Proteção de Informações Pessoais, o Decreto de Execução da mesma e os Padrões para Medidas que Garantam a Segurança de Informações Pessoais.

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

   a. Essas medidas técnicas e organizacionais estão descritas em mais detalhes no Anexo I deste Adendo.

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

4. **Incidente de Segurança.** O Fornecedor notificará a CHS imediatamente e, no máximo, 48 horas após a descoberta, por escrito, no caso de: (i) quaisquer Dados Pessoais sejam divulgados ou haja suspeita de que tenham sido divulgados pelo Fornecedor em violação ao Contrato Principal

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, 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

e/ou a este Adendo, ou às Leis de Privacidade de Dados aplicáveis ou (ii) o Fornecedor descubra, seja notificado ou suspeite que um Incidente de Segurança envolvendo Dados Pessoais tenha ocorrido, possa ter ocorrido ou possa ocorrer.

a. Se o Contrato Principal previr um contato específico da CHS, o Fornecedor notificará esse contato e também enviará uma notificação por e-mail para CHSinformationsecurity@chsinc.com. Se o Contrato ou outros termos e condições sob os quais o Fornecedor presta bens, serviços ou software para a CHS não preveem um contato específico, o Fornecedor notificará a Segurança da Informação da CHS por e-mail em CHSinformationsecurity@chsinc.com e/ou pelo telefone do Centro de Serviços de TI: 651-355-5555 ou 800-852-8185. O Fornecedor também fornecerá à CHS qualquer outro aviso exigido em lei.

b. O Fornecedor deverá cooperar plenamente na investigação do Incidente de Segurança, indenizar e reembolsar a CHS por todos e quaisquer danos, perdas, taxas, multas ou custos (sejam diretos, indiretos, especiais ou consequentes), incluindo honorários e custos advocatícios razoáveis, incorridos como resultado de tal incidente, e remediar qualquer dano ou potencial dano causado por tal incidente. Na medida em que um Incidente de Segurança dê origem a uma necessidade, a critério exclusivo da CHS, de fornecer (i) notificação a autoridades públicas, indivíduos ou outras pessoas, ou (ii) tomar outras medidas corretivas (incluindo, sem limitação, aviso, serviços de monitoramento de crédito e o estabelecimento de uma central de atendimento para responder a perguntas (cada uma das ações anteriores como "Ação(ões) Corretiva(s)"), a pedido da CHS, o Fornecedor deverá, a seu custo, tomar essas Ações Corretivas. efetuar quaisquer avisos serão determinados pela CHS a seu exclusivo critério.

c. Salvo exigência em lei ou exigência contrária de atuação urgente para mitigar ou evitar mais prejuízos ou danos a

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 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

pessoas ou bens, o Fornecedor não informará a qualquer terceiro sobre qualquer Incidente de Segurança sem primeiro obter a anuência prévia e escrita da CHS. Quando o Fornecedor informar a qualquer terceiros sobre um Incidente de Segurança, conforme exigido em lei ou de outra forma para atuação urgente para mitigar ou evitar mais prejuízos ou danos a pessoas ou bens, o Fornecedor entregará uma notificação à CHS em simultaneidade com qualquer outra notificação.

d. Na medida do razoavelmente solicitado pelo CHS, após a notificação de um Incidente de Segurança, a cooperação do Fornecedor com relação à investigação do Incidente de Segurança deverá incluir: (i) fornecer CHS acesso físico às instalações e operações afetadas; (ii) facilitar entrevistas com colaboradores do Fornecedor ou outros envolvidos na questão; e (iii) disponibilizar todos os registros, arquivos, relatórios de dados e outros materiais relevantes necessários para cumprir a lei, regulamento, normas industrias relevantes ou conforme razoavelmente exigido, de outra forma, pela CHS ou seus designados. O Fornecedor também deverá tomar medidas proativas para mitigar o risco de danos adicionais decorrentes do Incidente de Segurança, incluindo a implementação de quaisquer medidas exigidas por lei ou conforme orientado pela CHS.

5. Transferência Transfronteiriça de Dados Pessoais. O Fornecedor não processará os Dados Pessoais em uma jurisdição fora do local de Tratamento acordado sem o consentimento por escrito da CHS. Na medida em que os Dados Pessoais incluam informações sobre indivíduos localizados no Espaço Econômico Europeu ("EEE"), Reino Unido, Argentina ou Suíça, e o Fornecedor ou quaisquer subcontratados armazenem ou obtenham acesso a esses Dados Pessoais fora do EEE, Reino Unido, Argentina ou Suíça, o Fornecedor concorda em Processar esses Dados Pessoais de acordo com as Cláusulas Contratuais Padrão da UE para a Transferência de

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, 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

Dados Pessoais para Países Terceiros de acordo com a Decisão de Implementação da Comissão (UE) 2021/914, Módulo Dois, que é incorporado por referência neste documento ("Contrato de Operador Modelo" ou "SCC"), o Adendo de Transferência Internacional de Dados do Reino Unido ("Adendo do Reino Unido"), que é incorporado neste documento por referência, para Dados Pessoais aos quais se aplicam as leis de proteção de dados do Reino Unido, e para Dados Pessoais aos quais se aplicam as leis de proteção de dados da Suíça ou da Argentina, incluindo as alterações específicas das leis locais da Suíça ou da Argentina ao Contrato de Operador Modelo. Na medida em que os Dados Pessoais incluírem informações sobre indivíduos localizados no Brasil, e que estavam localizados no Brasil no momento em que as informações foram coletadas e o Fornecedor ou quaisquer subcontratados armazenarem ou, de outra forma, obtiverem acesso a esses Dados Pessoais fora do Brasil, o Fornecedor concorda em Tratar esses Dados Pessoais de acordo com as Cláusulas Modelo Brasileiras ("BMC"), conforme publicadas pela Autoridade Nacional de Proteção de Dados ("ANPD"), que são incorporadas aqui como Anexo II. Na medida em que o Fornecedor Processar Dados Pessoais em uma jurisdição específica que não seja o EEE, o Reino Unido, a Argentina ou a Suíça, e tal Tratamento for proibido pelas leis de privacidade aplicáveis na ausência da implementação de prazos comparáveis ao Contrato Modelo do Operador, o Fornecedor deverá Processar todos esses Dados Pessoais de acordo com o Contrato Modelo do Operador e, para tais fins, as referências às jurisdições da UE/EEE serão consideradas referências às jurisdições relevantes não pertencentes à UE/EEE, conforme aplicável.

a. Com relação ao Modelo de Contrato do Operador: (i) a assinatura deste Adendo constitui a assinatura do Contrato do Operador Modelo, incluindo os respectivos apêndices; (ii) cada uma das CHS e/ou subsidiárias da CHS estabelecidas no EEE, Reino Unido, Argentina ou Suíça será considerada, para os fins deste Adendo, como o "exportador de dados"; (iii) o Fornecedor e cada subcontratado que armazena, acessa ou de outra forma trata esses

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.

Dados Pessoais serão considerados, para os fins deste Adendo, como "importador de dados"; (iv) as atividades de Tratamento de dados no Anexo I do Contrato Modelo do Operador serão as descritas no Anexo 1 deste Adendo; e (v) as medidas de segurança de dados no Anexo II do Contrato Modelo do Operador serão as identificadas no Anexo I deste Adendo; e o(s) Contrato(s) Principal(is). Para os objetivos dos Adendos do Reino Unido: Para fins do Adendo do Reino Unido: (a) A Tabela 1 deverá ser preenchida com as informações relativas às partes estabelecidas no Apêndice 1; (b) A Tabela 2 deverá ser preenchida com as informações desta Cláusula; (c) A Tabela 3 deverá ser preenchida fazendo referência às informações correspondentes no Apêndice 1 e no Anexo I deste Adendo; e (d) Na Tabela 4, a opção "Exportador" deverá ser selecionada.

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

b. Com relação ao Contrato de Operador Modelo, o seguinte é reconhecido e acordado tanto pela CHS quanto pelo Fornecedor: (i) a Cláusula 7 da Cláusula de Ancoragem deverá ser aplicada; (ii) o exportador de dados deverá receber aviso prévio de 60 dias de acordo com a Cláusula 9(a); (iii) o Fornecedor deverá obter autorização específica (conforme detalhado acima na Cláusula 2(d) para a nomeação de suboperadores; (iv) o idioma opcional sob a Cláusula 11(a) (Recurso opcional com Órgão de Resolução Independente) não deverá ser aplicado; as partes escolhem a autoridade supervisora da Agência Espanhola de Proteção de Dados (AEPD); a lei regente com relação à Cláusula 17, Opção 1 (Lei Regente) será aplicada e o "Estado Membro" será a Espanha, o Contrato Modelo do Operador será regido pelas leis da jurisdição aplicável ao exportador da CHS; e (x) para fins da Cláusula 18 (Escolha de Foro e Jurisdição), quaisquer litígios decorrentes do Contrato Modelo do Operador serão resolvidos pelos tribunais da Espanha.

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.

c. As emendas da lei local suíça ao Contrato Modelo do Operador são as seguintes: 1. Autoridade de Supervisão O Comissário Federal de Proteção de Dados e Informações é a autoridade de supervisão competente; 2. Lei Aplicável para Reclamações Contratuais nos termos da Cláusula 17: Lei suíça (ou a lei de um país que permita e conceda direitos como terceiro beneficiário para reivindicações contratuais relativas a transferências de dados de acordo com a Lei Federal de Proteção de Dados "FADP"); 3. Estado-membro / União Europeia: A Suíça deve ser considerada como um Estado Membro dentro do significado do Contrato Modelo do Operador, de modo que os titulares dos dados, entre outros, tenham o direito de apresentar reclamações de acordo com a cláusula 18c do Contrato Modelo do Operador em sua residência habitual na Suíça; 4. As referências ao Regulamento Geral de Proteção de Dados e ao Regulamento (UE) 2016/679 devem ser entendidas como referências ao FADP; 5. Dados Pessoais: Dados Pessoais: Até a entrada em vigor da FADP revisada em 1º de setembro de 2023, que não protege mais dados de pessoas jurídicas, mas apenas dados de pessoas físicas, o Contrato Modelo do Operador também se aplica a dados de pessoas jurídicas.

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 subject. Supplier shall

d. Com relação aos Dados Pessoais de titulares de dados coreanos: O Fornecedor reconhece que as transferências internacionais de tais dados exigem notificação ao titular dos dados sobre: (i) os Dados Pessoais a serem transferidos; (ii) o país, a hora e o método de transferência; (iii) o nome e as informações de contato do destinatário; (iv) a finalidade de uso e o período de retenção pelo destinatário; e (v) o método e o procedimento para se opor à transferência e as consequências de tal objeção. O consentimento do titular dos dados para tais transferências também deverá ser obtido quando exigido pela lei aplicável, tal como quando a transferência não for necessária para que

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

a CHS execute seu contrato subjacente com o titular dos dados. O Fornecedor deverá auxiliar a CHS no cumprimento dessas obrigações.

e. Com relação aos Dados Pessoais de titulares de dados brasileiros: (i) o BMC deverá ser executado conforme previsto no Anexo II; (ii) cada uma das CHS e/ou subsidiárias da CHS estabelecidas no Brasil será considerada, para os fins deste Adendo, como o "exportador de dados"; (iii) o Fornecedor e cada subcontratado que armazene, acesse ou de outra forma trate tais Dados Pessoais serão considerados, para os fins deste Adendo, como "importador de dados"; (v) a ANPD é a autoridade supervisora competente nos termos do BMC; e (vi) no caso de qualquer disposição deste Anexo contradizer, direta ou indiretamente, o BMC, o BMC prevalecerá.

f. Com relação aos dados pessoais de titulares de dados argentinos: as alterações da lei local argentina ao Contrato Modelo do Operador são as seguintes: 1. "Lei de Privacidade de Dados" significa a Lei de Proteção de Dados Pessoais N.º 25.326 e Decreto Regulamentar N.º 1558/2001, conforme emendado, complementado e/ou substituído no futuro; "Dados Pessoais", "Dados Pessoais Sensíveis", "Tratamento", "Controlador" e "Titular dos Dados" terão o significado estabelecido na Lei de Privacidade de Dados; "autoridade" ou "autoridade supervisora" significará a Direção Nacional de Proteção de Dados Pessoais da Argentina; "exportador de dados" significa a parte responsável pelo Tratamento que transfere os Dados Pessoais; 'importador de dados' ou 'Operador' significa o prestador de serviços, conforme estabelecido na cláusula 25 da Lei de Privacidade de Dados, que está estabelecido fora da Argentina e concorda em receber do

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 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

exportador de dados os Dados Pessoais para Tratamento posterior, de acordo com os termos do Contrato Principal e deste Adendo; 2. Os Titulares dos Dados podem exigir que o importador de dados, como terceiros beneficiários, cumpra as disposições da Lei de Privacidade de Dados; 3. O importador de dados aceita que a autoridade supervisora exerça seus poderes dentro dos limites concedidos pela Lei de Privacidade de Dados, aceitando seus poderes de controle e sanção, concedendo à autoridade supervisora para tais fins, no que for pertinente, a capacidade de terceiro beneficiário; 4. O exportador de dados garante e se compromete que (i) informou aos Titulares dos Dados que seus Dados Pessoais poderão ser transferidos para um terceiro país que não ofereça um nível adequado de proteção de dados, (ii) se os Titulares dos Dados ou a autoridade supervisora - como terceiros beneficiários - exercerem seus direitos ou poderes, conforme o caso, o exportador de dados responderá à solicitação dentro dos termos estabelecidos pela Lei de Privacidade de Dados, e (iii) manterá uma lista de contratos de subprocessamento celebrados pelo importador de dados, que deverá ser atualizada pelo menos uma vez por ano, e que a lista estará disponível para a autoridade supervisora; 5. O importador de dados garante e se compromete que: (a) verificou que sua legislação local não impede o importador de dados de cumprir as obrigações, representações e princípios incluídos no Contrato Principal e no Adendo, e notificará prontamente o exportador de dados sobre a existência de qualquer disposição dessa natureza assim que tiver conhecimento; (b) notificará prontamente o exportador de dados sobre: (i) qualquer solicitação legalmente vinculante de divulgação dos Dados Pessoais emitida por uma autoridade de aplicação da lei, a menos que proibido de outra forma pelos regulamentos aplicáveis; (ii) todo acesso acidental ou

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 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.

não autorizado aos Dados Pessoais; e (iii) toda solicitação recebida diretamente dos Titulares dos Dados; (c) não cederá ou transferirá Dados Pessoais a terceiros, exceto se a cessão ou transferência for exigida por lei ou por uma autoridade competente, caso em que verificará se a autoridade solicitante oferece garantias adequadas de conformidade com os princípios da Lei de Privacidade de Dados e os direitos dos Titulares dos Dados; (d) tratará as solicitações e consultas recebidas dos Titulares dos Dados (ou do exportador de dados agindo em nome do Titular dos Dados) e da autoridade supervisora, que serão considerados como terceiros beneficiários; e (e) no caso de subprocessamento de Dados Pessoais, terá informado previamente o exportador de dados e obtido seu consentimento prévio por escrito; 6. O exportador de dados e o importador de dados concordam que, com relação ao Tratamento de Dados Pessoais, o Contrato Principal e o Adendo serão regidos pelas leis da Argentina e que, em caso de conflito relacionado à proteção de Dados Pessoais, a jurisdição judicial e administrativa da Argentina será competente; 7. O exportador de dados e o importador de dados concordam que, após a rescisão da prestação de serviços de Tratamento, o importador de dados e o subprocessador, se houver, deverão, a critério do exportador de dados, devolver todos os Dados Pessoais transferidos e suas cópias ao exportador de dados ou destruir todos os Dados Pessoais e certificar o mesmo.

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

6. Obrigações Diversas.

a. O Fornecedor deverá, mediante solicitação da CHS, executar prontamente contrato(s) de tratamento de dados suplementares com a CHS ou qualquer uma de suas subsidiárias, fornecer a assistência necessária ou tomar outras medidas apropriadas, com seus melhores esforços, para atender à transferência transfronteiriça e outros

agreement(s), assistances, and steps are necessary to address applicable Data Privacy Laws concerning Personal Data.

requisitos se a CHS concluir, a seu exclusivo critério, que esses contratos de tratamento de dados suplementares, assistências e medidas são necessários para atender às Leis de Privacidade de Dados aplicáveis relativas aos Dados Pessoais.

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.

b. O Fornecedor nomeará um responsável pela proteção de dados quando tal nomeação for exigida pelas leis de proteção de dados. O contato com a pessoa nomeada poderá ocorrer por e-mail, no endereço eletrônico fornecido pelo Fornecedor na página de assinaturas do presente DPA. O Fornecedor notificará imediatamente a CHS sobre qualquer alteração nas informações de contato do diretor de proteção de dados.

c. Supplier certifies that it understands and will comply, and cause all Supplier personnel to certify that they understand and will comply with the requirements of this Addendum.

c. O Fornecedor certifica que entende e cumprirá, e fará com que toda a equipe do Fornecedor certifique que entende e cumprirá os requisitos deste Adendo.

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.

d. As partes concordam que, na medida em que tal direito esteja claramente estabelecido no Contrato Principal, o Fornecedor poderá usar os Dados Pessoais da CHS em nome da CHS. Nesses casos, a CHS instrui o Fornecedor a usar apenas informações não identificadas ou agregadas e, para fins de clareza, a CHS instrui o Fornecedor a primeiro anonimizar, agregar e/ou desidentificar os Dados Pessoais conforme necessário para esse fim. Com relação a essas informações não identificadas ou agregadas: (1) O Fornecedor deverá cumprir todas as leis aplicáveis, incluindo a implementação de: (a) salvaguardas técnicas que proíbam a reidentificação; (b) tratamentos comerciais que proíbam especificamente a reidentificação; (c) tratamentos comerciais para evitar a liberação inadvertida de informações desidentificadas; e (2) o Fornecedor não fará nenhuma tentativa de reidentificar as informações.

e. At all times at which Supplier holds CHS's Personal Data, Supplier will have in place a bona fide business continuity

e. Sempre que o Fornecedor detiver Dados Pessoais da CHS, o Fornecedor terá implantado um plano de continuidade

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.

dos negócios de boa-fé que garantirá que o Fornecedor pode continuar os serviços na interrupção da prestação dos serviços por qualquer motivo fora do controle razoável do fornecedor ("Plano de Continuidade dos Negócios"). O Fornecedor deverá manter e atualizar o Plano de Continuidade dos Negócios, pelo menos, anualmente para cada um dos seus locais operacionais relacionados à prestação de serviços. O Fornecedor implantará o Plano de Continuidade dos Negócios se um local se tornar incapaz de executar esses serviços ou entregar serviços por um período maior que cinco (5) dias corridos. O Fornecedor executará uma avaliação hábil após a ocorrência de qualquer evento que venha a atrasar a execução da manutenção e suporte ou a entrega de serviços por um período maior que cinco (5) dias corridos. O Fornecedor ativará o Plano de Continuidade dos Negócios se o Fornecedor determinar que não conseguirá executar os serviços por um período maior que cinco (5) dias 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.

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.

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

7. **Lei Aplicável.** Este Adendo será regido e interpretado de acordo com as leis do estado que regem o Contrato Principal, sem levar em conta suas regras de escolha de lei.

8. **Prazo, Rescisão e Data de Vigência.**

a. Este Adendo entrará em vigor a partir da última data executada por uma das partes (a "Data de Vigência") e permanecerá em pleno vigor e efeito enquanto o(s) Contrato(s) Primário(s) permanecer(em) em vigor, a menos que seja rescindido antecipadamente de acordo com a Cláusula 8, alínea b).

b. A CHS poderá rescindir este Adendo e/ou o Contrato Primário imediatamente, sem aviso ou resolução judicial e sem prejuízo de quaisquer outros recursos, caso (i) o cumprimento dos termos deste Adendo pelo Fornecedor coloque o Fornecedor em violação de suas obrigações legais; (ii) o Fornecedor esteja em violação substancial de quaisquer declarações ou garantias dadas por ele nos termos deste Adendo e não consiga sanar tal violação com aviso prévio de (30) dias da CHS; (iii) o Fornecedor forneça aviso à CHS nos termos da Cláusula 2, alínea b) deste Adendo; (iv) uma autoridade de proteção de dados ou outra autoridade reguladora ou outro tribunal ou corte nos países em que a CHS ou suas subsidiárias operam constatarem que houve uma violação de quaisquer leis relevantes nessa jurisdição em virtude do Tratamento dos Dados Pessoais pelo Fornecedor ou pela CHS; ou (v) se qualquer uma das partes fizer uma cessão em benefício dos credores, ficar sujeita a um processo de falência, estiver sujeita à nomeação de um administrador judicial ou admitir por escrito sua incapacidade de pagar suas dívidas no vencimento.

c. Este Adendo será imediatamente rescindido se todos os Contratos Principais aplicáveis forem rescindidos por qualquer motivo

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

d. Após a rescisão deste Adendo por qualquer motivo, o Fornecedor devolverá todos os Dados Pessoais e todas as cópias dos Dados Pessoais sujeitos a este Adendo à CHS ou, a pedido da CHS, destruirá (ou seja, tornará as informações permanentemente ilegíveis e não reconstruíveis em um formato utilizável de acordo com os padrões atuais do Departamento de Defesa dos EUA ou do CESG, ou padrões equivalentes de destruição de dados, conforme aplicável) todos esses Dados Pessoais e certificará à CHS que o fez.

Página de assinatura a seguir

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

EM TESTEMUNHO DO QUE, as partes assinaram este Adendo e declaram que seus respectivos signatários, cujas assinaturas aparecem abaixo, estão autorizados por todas as ações corporativas necessárias para executar este Adendo.

Este Adendo pode ser assinado em uma ou mais vias, cada uma das quais será considerada um original, mas todas juntas constituirão um único e mesmo contrato.

Assinado por:
[Insira a Entidade CHS]

Assinatura

Nome

Data

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

Fornecedor

EM TESTEMUNHO DO QUE, as partes assinaram este Adendo e declaram que seus respectivos signatários, cujas assinaturas aparecem abaixo, estão autorizados por todas as ações corporativas necessárias para executar este Adendo.

Este Adendo pode ser assinado em uma ou mais vias, cada uma das quais será considerada um original, mas todas juntas constituirão um único e mesmo contrato.

Assinado por:
[Insira o nome do Fornecedor]

Assinatura

Nome

Data

Title	Cargo
Email Address of DPO, if applicable	Endereço de e-mail do DPO, se aplicável

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].*

APÊNDICE 1 ÀS CLÁUSULAS CONTRATUAIS PADRÃO DA UE

O presente Apêndice 1 inclui determinados detalhes do Tratamento dos Dados Pessoais da CHS (CHS Inc.) conforme exigido pelo Artigo 28(3) do GDPR (ou, quando aplicável, disposições equivalentes de qualquer outra Lei de Proteção de Dados).

Parte A. Lista das partes

EXPORTADORA DE DADOS
Nome: [Inserir a Entidade CHS]
Endereço: [Inserir o endereço da Entidade CHS]
Nome, cargo e detalhes de contato da pessoa de contato: [Inserir detalhes]
Atividades relevantes para os dados transferidos nos termos das SCCs: Conforme descrito no Contrato Principal
Assinatura e data: Veja as assinaturas e a(s) data(s) assinada(s) na página de assinatura do Adendo
Função: Controlador

IMPORTADORA DE DADOS
Nome: [Inserir o prestador de serviços].
Endereço: [Inserir o endereço do prestador de serviços].
Nome, cargo e detalhes de contato da pessoa de contato: [Inserir detalhes]
Atividades relevantes para os dados transferidos nos termos das SCCs: Conforme descrito no Contrato Principal
Assinatura e data: Veja as assinaturas e a(s) data(s) assinada(s) na página de assinatura do Adendo
Função: Operador

Parte B. Descrição da transferência

Categorias de titulares de dados cujos Dados Pessoais são transferidos:
- *[Inserir detalhes]*

Categorias de Dados Pessoais transferidos:
- *[Inserir detalhes]*

Categorias de dados confidenciais, incluindo medidas adicionais
- *[Inserir detalhes, se aplicável, ou marcar como N/A, se não for aplicável].*

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.

A frequência da transferência (por exemplo, se os dados são transferidos em uma base única ou contínua).

- Contínua

Natureza do Tratamento

- *[Inserir descrição geral dos Serviços de Processamento a serem fornecidos].*

Finalidade(s) da transferência de dados e do Tratamento posterior

- *[Inserir a descrição geral das finalidades para as quais os Dados Pessoais serão Tratados].*

O período pelo qual os Dados Pessoais serão retidos ou, se isso não for possível, os critérios usados para determinar esse período:

- *Os Dados Pessoais transferidos podem ser armazenados de forma identificável por um período não superior ao necessário para as finalidades para as quais os Dados Pessoais foram transferidos e, em nenhum caso, superior ao permitido pelas leis do país do exportador de dados.*

Para transferências para (sub) operadores, forneça uma lista de (sub) operadores:

- *[Inserir lista ou URL onde a lista de (sub) operadores possa ser visualizada].*

Para transferências para (sub) operadores, especifique também o assunto, a natureza e a duração do Tratamento

- *[Assunto, natureza e duração do Tratamento para transferências para o (sub) operador].*

Liste o país ou os países em que o importador de dados ou qualquer um de seus subprocessadores está Tratando os Dados Pessoais.

- *[Inserir lista].*

Parte C. Autoridade de supervisão competente A autoridade de supervisão competente é a autoridade de supervisão do Estado-Membro da UE/EEE onde o exportador de dados do CHS está estabelecido. Para transferências de dados no âmbito do FADP, é o Comissário Federal de Proteção de Dados e Informações.

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

ANEXO I - REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

Tendo em conta a natureza, o âmbito, o contexto e a finalidade do Tratamento, bem como os riscos para os direitos e liberdades dos indivíduos, o Fornecedor deverá implementar medidas físicas, técnicas e organizacionais adequadas para garantir um nível de segurança dos Dados Pessoais da CHS adequado ao risco, como se segue:

1. Segurança da Informação.

a. O Fornecedor implantará e manterá um programa escrito de segurança da informação, incluindo políticas, procedimentos e avaliações de risco apropriadas que sejam revisados, pelo menos, anualmente.

b. O Fornecedor implantará defesas administrativas, físicas e técnicas para:

i. Proteger os Dados Pessoais da CHS;de acesso não autorizado, exfiltração, aquisição ou divulgação, destruição, alteração, perda acidental, uso inadequado ou danos;

ii. O Fornecedor não utilizará ou armazenará quaisquer Dados Pessoais da CHS em software, modelos, algoritmos, hardware ou outras ferramentas ou ajudas de qualquer tipo, de autoaperfeiçoamento ou de aprendizado de máquina, e

iii. Tomará todas as medidas necessárias para mitigar danos, perdas, custos e despesas causados pelos eventos estabelecidos na Seção 4 deste Adendo.

c. O Fornecedor deverá notificar a CHS sobre quaisquer alterações significativas para as defesas administrativas, físicas ou técnicas que tenham expectativa razoável de afetar de forma negativa a proteção de Dados Pessoais da CHS; de acesso não autorizado, exfiltração, aquisição ou

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, 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

divulgação, destruição, alteração, perda acidental, uso inadequado ou danos.

d. Todos os direitos, títulos e interesses nos Dados Pessoais da CHS permanecerão como propriedade da CHS. O Fornecedor não tem direitos de propriedade intelectual ou qualquer outra reivindicação sobre os Dados Pessoais da CHS que estejam hospedados, armazenados ou transferidos de e para os sistemas e instalações do próprio Fornecedor ou de um provedor de nuvem hospedado por terceiros. Os Dados Pessoais do CHS não serão utilizados para fins analíticos, de marketing ou qualquer outro fim que não o uso pretendido estabelecido neste Contrato, ou para o benefício de qualquer outra pessoa que não a CHS.

e. Quando o Fornecedor receber, armazenar e/ou Tratar os Dados Pessoais dos CHS utilizando os próprios sistemas e instalações do Fornecedor, ou um provedor de nuvem hospedado por terceiros, o Fornecedor não deverá alterar a localização dos Dados Pessoais dos CHS ou do provedor de hospedagem designado sem a autorização dos CHS. No caso de o Fornecedor, por qualquer motivo, solicitar a alteração da região de hospedagem ou do provedor de hospedagem, o Fornecedor deverá fornecer à CHS um aviso com pelo menos sessenta (60) dias de antecedência a tal alteração. A CHS terá o direito de se opor a tal alteração solicitada e/ou rescindir o Contrato e este Adendo a seu exclusivo critério.

f. Quando o Fornecedor receber, armazenar e/ou tratar os Dados Pessoais da CHS usando os próprios sistemas e instalações do Fornecedor, o Fornecedor implementará e manterá os Controles Críticos do CIS (definidos como os Controles Críticos de Segurança do Centro de Segurança da Internet para uma Defesa Cibernética Eficaz), incluindo, mas

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 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

não se limitando aos seguintes controles, cada um deles conforme explicado mais detalhadamente nos Controles Críticos do CIS, como segue:

i. Inventário e Controle de Ativos Empresariais. Gerencie ativamente (inventarie, rastreie e corrija) todos os ativos da empresa (dispositivos de usuário final, inclusive portáteis e móveis; dispositivos de rede; dispositivos que não sejam de computação/Internet das Coisas (IoT); e servidores) conectados à infraestrutura física, virtual, remotamente e aqueles em ambientes de nuvem, para conhecer com precisão a totalidade dos ativos que precisam ser monitorados e protegidos na empresa. Isso também ajudará a identificar ativos não autorizados e não gerenciados a serem removidos ou corrigidos.

ii. Inventário de Softwares Autorizados e Não Autorizados. Gerenciar ativamente (realizar inventário, rastrear e corrigir) todos os softwares na rede para que somente os softwares autorizados sejam instalados e possam operar e assegurar que os softwares não autorizados e não gerenciados sejam encontrados e tenham sua instalação ou execução impedida.

iii. Configuração Segura de Ativos e Software da Empresa. Estabeleça e mantenha a configuração segura dos ativos da empresa (dispositivos do usuário final, inclusive portáteis e móveis; dispositivos de rede; dispositivos que não sejam de

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

computação/IoT; e servidores) e do software (sistemas operacionais e aplicativos).

iv. Gerenciamento Contínuo de Vulnerabilidades. Desenvolva um plano para avaliar e rastrear continuamente as vulnerabilidades em todos os ativos da empresa dentro da infraestrutura da empresa, a fim de remediar e minimizar a janela de oportunidade para os invasores. Monitore fontes públicas e privadas do setor para obter novas informações sobre ameaças e vulnerabilidades.

v. Gerenciamento de Registros de Auditoria. Colete, alerte, analise e retenha registros de auditoria de eventos que possam ajudar a detectar, entender ou se recuperar de um ataque.

vi. Proteções de E-mail e Navegador. Minimizar a superfície de ataque e as oportunidades para que invasores manipulem o comportamento humano através de sua interação com navegadores e sistemas de e-mail.

vii. Defesas contra Malware. Impeça e controle a instalação, a disseminação e a execução de aplicativos, códigos ou scripts maliciosos nos ativos da empresa.

viii. Gerenciamento da Infraestrutura de Rede. Estabeleça, implemente e gerencie ativamente (rastreie, informe, corrija) os dispositivos de rede para evitar que os invasores explorem serviços de rede e pontos de acesso vulneráveis.

ix. Recuperação de Dados. Estabelecer e manter práticas

practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

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.

de recuperação de dados suficientes para restaurar os ativos da empresa no escopo para um estado confiável e anterior ao incidente.

x. Monitoramento e Defesa da Rede. Opere tratamentos e ferramentas para estabelecer e manter um monitoramento de rede abrangente e a defesa contra ameaças à segurança em toda a infraestrutura de rede e base de usuários da empresa.

xi. Proteção de Dados. Desenvolver processos e controles técnicos para identificar, classificar, tratar, reter e descartar dados com segurança.

xii. Gerenciamento de Contas. Use processos e ferramentas para atribuir e gerenciar a autorização de credenciais para contas de usuário, incluindo contas de administrador, bem como contas de serviço, para ativos e software da empresa.

xiii. Gerenciamento de Controle de Acesso. Use processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais e privilégios de acesso para contas de usuário, administrador e serviço para ativos e software corporativos.

xiv. Conscientização sobre Segurança e Treinamento de Habilidades. Estabeleça e mantenha um programa de conscientização de segurança para influenciar o comportamento da força de trabalho, para que ela se conscientize sobre a segurança e tenha as habilidades adequadas para reduzir os riscos de segurança

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 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.

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-

cibernética para a empresa.

xv. Segurança do Software do Aplicativo. Gerenciar o ciclo de vida da segurança de todos os softwares desenvolvidos internamente, hospedados e adquiridos para prevenir, detectar e corrigir os pontos fracos da segurança antes que eles possam afetar a empresa.

xvi. Gerenciamento de Resposta a Incidentes. Estabeleça um programa para desenvolver e manter uma capacidade de resposta a incidentes (por exemplo, políticas, planos, procedimentos, funções definidas, treinamento, comunicações) para preparar, detectar e responder rapidamente a um ataque.

xvii. Teste de Penetração. Teste a eficácia e a resiliência dos ativos da empresa por meio da identificação e da exploração de pontos fracos nos controles (pessoas, tratamentos e tecnologia) e da simulação dos objetivos e das ações de um invasor.

xviii. Gerenciamento de Fornecedores. Desenvolva um processo para avaliar os prestadores de serviços que detêm dados confidenciais ou são responsáveis por plataformas ou processos críticos de TI de uma empresa, para garantir que esses prestadores estejam protegendo essas plataformas e dados adequadamente.

2. Auditorias

a. A CHS deverá tratar qualquer um dos relatórios de auditoria a seguir ou outros relatórios de auditoria como informações confidenciais do Fornecedor para fins de obrigações de

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

   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

confidencialidade, se houver, nos termos de qualquer(is) contrato(s) então existente(s) entre o Fornecedor e a CHS. O fornecedor corrigirá prontamente qualquer exceção ou falha observada em qualquer relatório de auditoria independente padrão do setor.

b. O Fornecedor, em relação a cada sistema que detém contém ou Trata Dados Pessoais da CHS:

   i. Realizar exames por um ou mais terceiros qualificados, conforme declarado e contemplado por um relatório de Controles da Organização de Serviços ("SOC") ou um relatório de auditoria independente padrão do setor emitido por esses terceiros, atestando que a descrição do sistema do Fornecedor feita pela gerência do Fornecedor apresenta de forma justa o sistema que foi projetado e implementado, em uma data específica não anterior a um ano antes da data de determinação (no caso de um relatório Tipo 1) ou implementado em um período de tempo especificado que inclua uma data não anterior a um ano antes da data de determinação (no caso de um relatório Tipo 2); e

   ii. Enquanto esse sistema detiver, contiver ou tratar os Dados Pessoais da CHS, fazer com que o sistema esteja em conformidade, em todos os aspectos materiais, com as afirmações da gerência em relação ao sistema sobre o qual o relatório SOC mais recente ou um relatório de auditoria independente padrão do setor e uma carta de ponte ou lacuna que cubra o período entre a expiração do relatório

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

anterior e a publicação do novo relatório.

c. Os Fornecedores, mediante solicitação da CHS, disponibilizarão à CHS para revisão, conforme aplicável, o mais recente Relatório de Conformidade da Indústria de Cartões de Pagamento ("PCI") do Fornecedor, o relatório de auditoria SOC ou quaisquer relatórios de auditoria independentes padrão do setor ou certificações realizadas pelo Fornecedor ou em seu nome, avaliando a eficácia do programa de segurança da informação do Fornecedor, conforme relevante para os Dados Pessoais da CHS.

   i. SOX: Se o Fornecedor estiver no escopo da conformidade da CHS com a Lei Sarbanes-Oxley (a "Lei SOX"), conforme possa ser alterada de tempos em tempos, o Fornecedor fornecerá anualmente à CHS, para revisão, o último Relatório SOC do Fornecedor enquanto o sistema detiver, contiver ou tratar os Dados Pessoais da CHS, ou

   ii. PCI: O Fornecedor fornecerá anualmente à CHS, para revisão, o(s) mais recente(s) Relatório(s) de Conformidade com o PCI e/ou relatório SOC do Fornecedor, enquanto o sistema detiver, contiver ou tratar os Dados Pessoais da CHS.

d. A pedido da CHS, para confirmar a conformidade do Fornecedor com o presente Adendo e quaisquer leis, regulamentos e padrões industriais aplicáveis, o Fornecedor permitirá que a CHS ou os agentes da CHS executem uma avaliação, auditoria, exame ou revisão de todos os controles no ambiente físico e/ou técnico do Fornecedor em relação a todos os Dados Pessoais da CHS sendo manejados, recebidos ou adquiridos

Agreement and this Addendum. Supplier shall cooperate fully with such assessment by providing access to knowledgeable personnel, physical premises, documentation, 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

e/ou serviços sendo prestados à CHS nos termos do acordo aplicável e do presente Adendo de Privacidade. O Fornecedor deverá cooperar de forma integral com a avaliação provendo acesso ao pessoal com conhecimento, premissas físicas, documentação, infraestrutura e softwares aplicáveis que tratam, armazenam ou transportam os Dados Pessoais da CHS para a CHS, conforme o acordo aplicável e o presente Adendo. Além disso, a pedido da CHS, o Fornecedor deverá fornecer à CHS os resultados de qualquer auditoria realizada por ou em nome do Fornecedor que avaliam a eficácia do programa de segurança de informação do Fornecedor como relevante à segurança e à confidencialidade dos Dados Pessoais da CHS compartilhados durante o curso do acordo aplicável e do presente Adendo.

e. PCI DSS.
    i. Definições.
        1. "Dados do Titular do Cartão" tem o significado atribuído a esse termo pelo PCI DSS ou por qualquer norma sucessora.
        2. "PCI DSS" significa o então atual Padrão de Segurança de Dados da Indústria de Cartões de Pagamento, conforme promulgado pelo Conselho de Normas de Segurança da PCI.
        3. "Fornecedor PCI" significa um provedor de serviços PCI conforme definido pelo PCI DSS.
        4. "AOC" significa o formulário do PCI Security Standard Council para comerciantes e prestadores de

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 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

serviços atestarem os resultados de uma avaliação do PCI DSS;

ii. Se, e na medida em que, qualquer um dos Dados Pessoais da CHS for um Dado do Titular do Cartão que o Fornecedor recebe ou trata como um Fornecedor PCI, o Fornecedor irá, a menos que expressamente permitido de outra forma por escrito pela CHS:

iii. Manter avaliações atualizadas e todas as outras qualificações e certificações necessárias para essa designação de acordo com o PCI DSS;

iv. Entregar à CHS o AOC do Fornecedor imediatamente após sua conclusão, na forma e contendo as informações exigidas pelo PCIDSS, com data não superior a um ano após o AOC anterior (se houver) entregue pelo Fornecedor à CHS;

v. Fornecer à CHS uma matriz de responsabilidade acordada identificando quais requisitos do PCI DSS serão gerenciados pelo Fornecedor; e

vi. De outra forma, cumprirá todos os requisitos do PCI DSS em relação aos Dados do Titular do Cartão.

3. Acesso aos Sistemas de Informações da CHS

a. Uso de Sistemas Permitidos. O Fornecedor utilizará quaisquer Sistemas Permitidos exclusivamente para executar as obrigações do Fornecedor à CHS. O Fornecedor não usará Sistemas Permitidos para nenhum outro objetivo.

b. Condições de Uso. O Fornecedor utilizará os Sistemas Permitidos exclusivamente de acordo com os termos do(s) acordo(s) em vigor entre

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.

a CHS e o Fornecedor e com as condições e políticas adicionais que a CHS disponibilizar ao Fornecedor periodicamente. Essas condições e políticas de uso poderão incluir (e ser descritas como) políticas, procedimentos, requisitos técnicos e/ou protocolos. A CHS poderá monitorar o acesso e as atividades do pessoal autorizado do Fornecedor nos Sistemas Permitidos da CHS.

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.

c. Acesso por Pessoal Autorizado do Fornecedor. O Fornecedor limitará acesso aos Sistemas Permitidos às Pessoas Autorizadas do Fornecedor. O Fornecedor proverá à CHS o nome de cada Pessoa Autorizada do Fornecedor. Cada Pessoa Autorizada do Fornecedor deve estabelecer e manter um identificador único para acesso e seguir as mesmas regras de segurança como pessoal da CHS. O Fornecedor deverá garantir que as pessoas físicas diferentes das Pessoas Autorizadas do Fornecedor (incluindo, entre outros, ex-funcionários e atuais funcionários que não têm função ativa na provisão de mercadorias, serviços ou softwares à CHS ou suas Afiliadas) não tenham acesso aos Sistemas de Informações da CHS. O Fornecedor permanecerá responsável por todas as ações e omissões de tal pessoal autorizado do Fornecedor.

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, 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)

d. Proibições Específicas. Exceto quando expressamente autorizado pela CHS por escrito e assinado (seja em uma declaração de trabalho, especificação de projeto, ordem de serviço ou direção escrita separada), o Fornecedor não deverá (i) tentar fazer engenharia reversa, desmontar, traduzir reversamente, descompilar ou de qualquer outra forma decodificar qualquer elemento dos Sistemas de Informação da CHS; (ii) tentar decifrar informações criptografadas ou codificadas; (iii) fazer modificações, aprimoramentos, adaptações ou traduções, no todo ou em parte, de

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.

qualquer elemento dos Sistemas de Informação da CHS, não autorizados pela CHS; (iv) acessar qualquer Sistema de Informação da CHS além da permissão expressamente concedida pela CHS; (v) fazer cópias de qualquer elemento dos Sistemas de Informação da CHS; (vi) usar qualquer Sistema de Informação da CHS ou dados para construir um produto ou serviço competitivo, ou de outra forma para fins comerciais; (vii) sondar computadores ou redes host; (viii) violar ou examinar os controles de segurança de um computador host, componente de rede ou sistema de autenticação, ou contornar ou divulgar a autenticação do usuário do Sistema de Informações da CHS ou controles de segurança; (ix) monitorar dados em qualquer rede ou sistema sem a autorização por escrito da CHS; (x) interferir ou interromper o serviço de qualquer usuário, host ou rede, ou sobrecarregar um servidor, dispositivo conectado à rede ou componente de rede ou ameaçar danos à propriedade; (xi) originar dados malformados ou tráfego de rede que resultem em danos ou interrupção de um serviço ou dispositivo conectado à rede; (xii) forjar dados ou deturpar a origem de um usuário ou fonte; (xiii) tomar qualquer ação que seja ilegal, abusiva, maliciosa, assediadora, tortuosa, difamatória, caluniosa ou invasiva do direito de privacidade de outra pessoa ou que infrinja os direitos de propriedade intelectual de qualquer pessoa; (xiv) violar qualquer lei ou regulamento aplicável; (xv) permitir o acesso de um concorrente da CHS. Caso o pessoal autorizado do Fornecedor tome qualquer medida que viole esta cláusula, a CHS poderá exigir que o Fornecedor substitua o pessoal autorizado do Fornecedor por outro pessoal autorizado do Fornecedor ou suspenda ou rescinda o Contrato Principal, declaração de trabalho ou pedido, a seu exclusivo

critério, preservando qualquer outro recurso disponível para a CHS.

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

e. Falha de Acesso. O Fornecedor reconhece que o acesso aos Sistemas Permitidos poderão ser interrompidos devido a circunstâncias dentro ou fora do controle razoável da CHS. Nada contido no presente Adendo ou em qualquer acordo entre o Fornecedor e a CHS será uma promessa ou compromisso de entrega de acesso aos Sistemas Permitidos ou que qualquer Sistema Permitido estará funcional. Apesar do acesso previsto nos termos do presente Adendo, nenhuma licença sob qualquer patente, direito autoral ou qualquer outro direito de propriedade intelectual relacionado ao Sistema de Informações da CHS é outorgada ao Fornecedor em virtude do acesso aos Sistemas Permitidos.

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.

f. Renúncia de Responsabilidade. A CHS exclui todas as declarações, garantias e compromissos, expressos ou implícitos, da CHS ou Afiliadas da CHS em relação aos Sistemas de Informações da CHS, incluindo, entre outros, quaisquer declarações, garantias ou condições de precisão, suficiência, adequação ou não violação relacionadas ao acesso ou uso de qualquer Sistema Permitido pelo Fornecedor. A CHS não terá qualquer responsabilidade por quaisquer danos, prejuízos ou despesas incorridas pelo Fornecedor em decorrência do acesso do Fornecedor ou Pessoas Autorizadas do Fornecedor aos Sistemas Permitidos (incluindo, entre outros, o acesso inadvertido de um vírus de computador ou outro arquivo ou programa de computador nocivo) ou de não disponibilização ou acessibilização do(s) Sistema(s) Permitido(s).

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

g. Sistemas do Fornecedor. Quando o Fornecedor acessar os Sistemas Permitidos com uso de hardware, software ou redes do Fornecedor, as seguintes disposições se aplicarão.

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 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).

i. Segurança de Acesso. O Fornecedor deverá garantir que as Pessoas Autorizadas do Fornecedor obtenham acesso aos Sistemas Permitidos através de um sistema de informática que mantém controles de autenticação e inclui um firewall adequado. O Fornecedor deverá seguir todas as regras e procedimento de segurança da CHS para restrição de acesso a seus sistemas de informática.

ii. Muro de Segregação. O Fornecedor garantirá que o pessoal autorizado do Fornecedor seja efetivamente isolado de seu pessoal que seja designado para a conta de um concorrente conhecido ou potencial da CHS ou das Afiliadas da CHS. O Fornecedor estabelecerá e documentará procedimentos físicos e eletrônicos para segregar e proteger todas as informações, dados e comunicações (incluindo, entre outros, os Dados Pessoais da 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:	

CLAUSE 3. Onward Transfers

OPTION A. 3.1. The Importer may not carry out an Onward Transfer of Personal Data subject to the

iii. ANEXO II - CLÁUSULAS MODELO BRASILEIRAS

CLÁUSULA 1. Identificação das Partes

1.1. Pelo presente contrato, o Exportador e o Importador (doravante, "Partes"), abaixo identificados, concordaram com as presentes cláusulas contratuais padrão (doravante, "Cláusulas") aprovadas pela Autoridade Nacional de Proteção de Dados (ANPD), para reger a Transferência Internacional de Dados descrita na CLÁUSULA 2, de acordo com as disposições da Legislação Nacional.

Nome: Qualificação: [Entidade CHS] Endereço principal: Endereço de e-mail: Contato para o Titular dos Dados: Outras informações:	

(x) Exportador/Controlador

Nome: Qualificação: Endereço principal: Endereço de e-mail: Contato para o Titular dos Dados: Outras informações:	

(x) Importador/Operador

CLÁUSULA 2. Objeto

2.1 Estas Cláusulas se aplicam às Transferências Internacionais de Dados Pessoais entre Exportadores de Dados e Importadores de Dados, conforme descrito abaixo.

Descrição da transferência internacional de dados:

Principais finalidades da transferência: Categorias de dados pessoais transferidos: Período de armazenamento dos dados: Outras informações:	

CLÁUSULA 3. Transferências Subsequentes

OPÇÃO A. 3.1. O Importador não poderá realizar uma Transferência Subsequente de Dados Pessoais sujeita à

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.

Transferência Internacional de Dados regida por estas Cláusulas, exceto nos casos previstos no item 18.3.

OPÇÃO B. 3.1. O Importador poderá realizar uma Transferência Subsequente de Dados Pessoais sujeita à Transferência Internacional de Dados regida por estas Cláusulas, nos casos e de acordo com as condições descritas abaixo e com o disposto na CLÁUSULA 18.

Principais finalidades da transferência: Categorias de dados pessoais transferidos: Período de armazenamento dos dados: Outras informações:	Principais finalidades da transferência: Categorias de dados pessoais transferidos: Período de armazenamento dos dados: Outras informações:

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:

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

CLÁUSULA 4. Responsabilidades das Partes

4.1 Sem prejuízo do dever de assistência mútua e das obrigações gerais das Partes, a Parte Designada abaixo, na qualidade de Controlador, será responsável pelo cumprimento das seguintes obrigações estabelecidas nestas Cláusulas:

a) Responsável pela publicação do documento previsto na CLÁUSULA 14:

( ) Exportador ( ) Importador

b) Responsável por responder às solicitações dos Titulares dos Dados de que trata a CLÁUSULA 15:

( ) Exportador ( ) Importador

c) Responsável por notificar o incidente de segurança previsto na CLÁUSULA 16:

( ) Exportador ( ) Importador

4.2. Para os fins destas Cláusulas, caso a Parte Designada nos termos do item 4.1. seja o Operador, o Controlador permanece responsável por:

a) cumprimento das obrigações previstas nas CLÁUSULAS 14, 15 e 16 e demais disposições estabelecidas na Legislação Nacional, especialmente em caso de omissão ou descumprimento das obrigações pela Parte Designada;

b) cumprimento das determinações da ANPD; e

c) guaranteeing the Data Subjects' rights and repairing damages caused, subject to the provisions of Clause 17.

c) garantir os direitos dos Titulares dos Dados e reparar os danos causados, observado o disposto na Cláusula 17.

SECTION II – MANDATORY CLAUSES

SEÇÃO II - CLÁUSULAS OBRIGATÓRIAS

CLAUSE 5 Purpose

CLÁUSULA 5 Objetivo

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.

5.1 Estas Cláusulas são apresentadas como um mecanismo para permitir o fluxo internacional seguro de dados pessoais, estabelecem garantias mínimas e condições válidas para a realização da Transferência Internacional de Dados e visam garantir a adoção de salvaguardas adequadas para o cumprimento dos princípios, dos direitos do Titular dos Dados e do regime de proteção de dados previstos na Legislação Nacional.

CLAUSE 6. Definitions

CLÁUSULA 6. Definições

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:

6.1 Para os fins destas Cláusulas, as definições do art. 5 da LGPD, e art. 3 do Regulamento sobre Transferência Internacional de Dados Pessoais serão consideradas, sem prejuízo de outros atos normativos emitidos pela ANPD. As Partes também concordam em considerar os termos e seus respectivos significados, conforme estabelecido abaixo:

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;
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

a) Agentes de tratamento: o controlador e o operador;
b) ANPD: Autoridade Nacional de Proteção de Dados;
c) Cláusulas: as cláusulas contratuais padrão aprovadas pela ANPD, que fazem parte das SEÇÕES I, II e III;
d) Contrato Relacionado: instrumento contratual firmado entre as Partes ou, no mínimo, entre uma delas e um terceiro, inclusive um Terceiro Controlador, que tenha finalidade comum, vínculo ou relação de dependência com o contrato que rege a Transferência Internacional de Dados;
e) Controlador: Parte ou terceiro ("Terceiro Controlador") responsável pelas decisões relativas ao tratamento de Dados Pessoais;
f) Dados Pessoais: informações relacionadas a uma pessoa física identificada ou identificável;
g) Dados Pessoais Sensíveis: dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato

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

ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, sempre que relacionados a uma pessoa natural;

h) Apagamento: exclusão de dados ou conjunto de dados de um banco de dados, independentemente do procedimento utilizado;

i) Exportador: agente de tratamento, localizado no território nacional ou em um país estrangeiro, que transfere dados pessoais para o Importador;

j) Importador: agente de tratamento, localizado em um país estrangeiro, que recebe dados pessoais do Exportador;

k) Legislação Nacional: conjunto de disposições constitucionais, legais e regulamentares brasileiras relativas à proteção de Dados Pessoais, incluindo a LGPD, o Regulamento de Transferência Internacional de Dados e outros atos normativos emitidos pela ANPD;

l) Lei de Arbitragem: Lei n.º 9.307, de 23 de setembro de 1996;

m) Medidas de Segurança: medidas técnicas e administrativas capazes de proteger os Dados Pessoais contra acesso não autorizado e contra eventos acidentais ou ilícitos de destruição, perda, alteração, comunicação ou difusão;

n) Órgão de Pesquisa: órgão ou entidade dos órgãos públicos ou entidades associadas ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no território brasileiro, que inclua pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico em sua missão institucional ou em seus objetivos sociais ou estatutários;

o) Operador: Parte ou terceiro, incluindo um Subprocessador, que trata os Dados Pessoais em nome do Controlador;

p) Parte Designada: Parte ou um Terceiro Controlador, nos termos da CLÁUSULA 4, designado para cumprir obrigações específicas relativas à transparência, aos direitos dos Titulares dos Dados e à notificação de incidentes de segurança;

q) Partes: Exportador e Importador;

r) Solicitação de Acesso: pedido de cumprimento obrigatório, por força de lei, regulamento ou determinação de autoridade pública, para

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.

conceder acesso aos Dados Pessoais objeto da Transferência Internacional de Dados regida por estas Cláusulas;

s) Subprocessador: agente de tratamento contratado pelo Importador, sem vínculo com o Exportador, para tratar os Dados Pessoais após uma Transferência Internacional de Dados;

t) Titular dos Dados: pessoa física a quem se referem os Dados Pessoais objeto da Transferência Internacional de Dados regida por estas Cláusulas;

u) Transferência: modalidade de tratamento pela qual um agente de tratamento transmite, compartilha ou fornece acesso a Dados Pessoais a outro agente de tratamento;

v) Transferência Internacional de Dados: transferência de Dados Pessoais para um país estrangeiro ou para uma organização internacional da qual o Brasil seja membro; e

w) Transferência Subsequente: transferência de Dados Pessoais, dentro do mesmo país ou para outro país, por um Importador para um terceiro, incluindo um Subprocessador, desde que não constitua uma Solicitação de Acesso.

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.

CLÁUSULA 7. Legislação Aplicável e supervisão da ANPD

7.1. A Transferência Internacional de Dados objeto destas Cláusulas estará sujeita à Legislação Nacional e à fiscalização da ANPD, inclusive com o poder de aplicar medidas preventivas e sanções administrativas a ambas as Partes, conforme o caso, bem como o poder de limitar, suspender ou proibir as transferências internacionais decorrentes deste acordo ou de um 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 is most in line with the National Legislation shall apply;

CLÁUSULA 8. Interpretação

8.1. Qualquer aplicação destas Cláusulas deverá ocorrer de acordo com os seguintes termos:

a) estas Cláusulas deverão sempre ser interpretadas de forma mais favorável ao Titular dos Dados e de acordo com as disposições da Legislação Nacional;

b) em caso de dúvida sobre o significado de qualquer termo destas Cláusulas, será aplicado o significado que estiver mais de acordo com a Legislação Nacional;

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.

c) nenhum item destas Cláusulas, incluindo um Acordo Relacionado e as disposições previstas na SEÇÃO IV, deverá ser interpretado como limitando ou excluindo a responsabilidade de qualquer das Partes em relação às obrigações previstas na Legislação Nacional; e

d) as disposições das SEÇÕES I e II prevalecerão em caso de conflito de interpretação com cláusulas adicionais e outras disposições estabelecidas nas SEÇÕES III e IV deste contrato ou em Acordos 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 Adesão

9.1. Por acordo mútuo entre as Partes, será possível a um agente de tratamento aderir a estas Cláusulas, seja como Exportador de Dados ou como Importador de Dados, mediante o preenchimento e a assinatura de um documento escrito, que fará parte deste contrato.

9.2 A parte aderente terá os mesmos direitos e obrigações que as partes originárias, de acordo com a posição assumida de Exportador ou Importador e de acordo com a categoria correspondente de agente de tratamento.

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;

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

CLÁUSULA 10. Obrigações Gerais das Partes

10.1. As Partes se comprometem a adotar e, quando necessário, demonstrar a implementação de medidas efetivas capazes de demonstrar a observância e o cumprimento do disposto nestas Cláusulas e na Legislação Nacional, bem como a eficácia de tais medidas e, em especial

a) utilizar os Dados Pessoais apenas para as finalidades específicas descritas na CLÁUSULA 2, sem possibilidade de tratamento posterior incompatível com tais finalidades, observadas as limitações, garantias e salvaguardas previstas nestas Cláusulas;
b) garantir a compatibilidade do tratamento com as finalidades informadas ao Titular dos Dados, de acordo com o contexto da atividade de tratamento;
c) limitar a atividade de tratamento ao mínimo necessário para o cumprimento de suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de Dados Pessoais;
d) garantir aos Titulares dos Dados, sujeito às

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.

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.

disposições da Cláusula 4: (d.1.) informações claras, precisas e de fácil acesso sobre as atividades de tratamento e os respectivos agentes de tratamento, observado o sigilo comercial e industrial; (d.2.) consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integridade de seus Dados Pessoais; e (d.3.) exatidão, clareza, pertinência e atualização dos Dados Pessoais, de acordo com a necessidade e para cumprimento da finalidade de seu tratamento;

e) adotar as medidas de segurança adequadas e compatíveis com os riscos envolvidos na Transferência Internacional de Dados regida por estas Cláusulas;

f) não tratar os Dados Pessoais para fins abusivos ou discriminatórios ilegais;

g) garantir que qualquer pessoa que atue sob sua autoridade, incluindo subprocessadores ou qualquer agente que colabore com eles, seja mediante remuneração ou gratuitamente, somente trate os dados pessoais em conformidade com suas instruções e com as disposições destas Cláusulas;

h) manter um registro das operações de tratamento de Dados Pessoais da Transferência Internacional de Dados regida por estas Cláusulas, e apresentar a documentação pertinente à ANPD, quando solicitado.

CLÁUSULA 11. Dados Pessoais Sensíveis

11.1. Se a Transferência Internacional de Dados envolver Dados Pessoais Sensíveis, as Partes deverão aplicar salvaguardas adicionais, incluindo Medidas de Segurança específicas que sejam proporcionais aos riscos da atividade de tratamento, à natureza específica dos dados e aos interesses, direitos e garantias a serem protegidos, conforme descrito na SEÇÃO III.

CLÁUSULA 12. Dados pessoais de crianças e adolescentes

12.1. Caso a Transferência Internacional de Dados regida por estas Cláusulas envolva Dados Pessoais relativos a crianças e adolescentes, as Partes deverão implementar medidas para garantir que o tratamento seja realizado em seu melhor interesse, nos termos da Legislação Nacional e dos instrumentos relevantes de direito internacional.

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.

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.

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

CLÁUSULA 13. Uso legal dos dados

13.1. O Exportador garante que os Dados Pessoais foram coletados, tratados e transferidos para o Importador de acordo com a Legislação Nacional.

CLÁUSULA 14. Transparência

14.1. A Parte Designada publicará, em seu site, um documento contendo informações facilmente acessíveis, escritas em linguagem simples, clara e precisa sobre a realização da Transferência Internacional de Dados, incluindo, no mínimo, informações sobre:

a) a forma, a duração e a finalidade específica da transferência internacional;
b) o país de destino dos dados transferidos;
c) a identificação e os detalhes de contato da Parte Designada;
d) o uso compartilhado de dados pelas Partes e sua finalidade;
e) as responsabilidades dos agentes que conduzirão o tratamento;
f) os direitos do Titular dos Dados e os meios para exercê-los, incluindo um canal de fácil acesso disponibilizado para responder às suas solicitações e o direito de registrar uma petição contra o Exportador e o Importador perante a ANPD; e
g) Transferências Subsequentes, incluindo aquelas relacionadas aos destinatários e à finalidade de tal transferência.

14.2. O documento a que se refere o item 14.1. deverá ser disponibilizado em página específica do site ou integrado, de forma destacada e de fácil acesso, à Política de Privacidade ou documento equivalente.

14.3. Mediante solicitação, as Partes disponibilizarão gratuitamente uma cópia destas Cláusulas ao Titular dos Dados, observado o sigilo comercial e industrial.

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;
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,

14.4. Todas as informações disponibilizadas aos Titulares dos Dados, nos termos destas Cláusulas, deverão ser redigidas em português.

CLÁUSULA 15. Direitos dos titulares dos dados

15.1. O Titular dos Dados terá o direito de obter da Parte Designada, no que diz respeito aos Dados Pessoais sujeitos à Transferência Internacional de Dados regida por estas Cláusulas, a qualquer momento e mediante solicitação, nos termos da Legislação Nacional:

a) confirmação da existência de tratamento;
b) acesso aos dados;
c) correção de dados incompletos, imprecisos ou desatualizados;
d) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com estas Cláusulas e com o disposto na Legislação Nacional;
e) portabilidade dos dados para outro prestador de serviços ou produtos, mediante solicitação expressa, de acordo com as normas da ANPD, observado o sigilo comercial e industrial;
f) eliminação dos Dados Pessoais tratados com o consentimento do Titular dos Dados, exceto nas hipóteses previstas na CLÁUSULA 20;
g) informações sobre entidades públicas e privadas com as quais as Partes tenham compartilhado dados;
h) informações sobre a possibilidade de negar o consentimento e sobre as consequências da negativa;
i) retirada do consentimento por meio de um procedimento gratuito e facilitado, restando ratificadas as atividades de tratamento realizadas antes do pedido de eliminação;
j) revisão das decisões tomadas exclusivamente com base no tratamento automatizado de dados pessoais que afetem seus interesses, incluindo decisões destinadas a

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

definir seu perfil pessoal, profissional, de consumo e de crédito ou aspectos de sua personalidade; e

k) informações sobre os critérios e procedimentos adotados para a decisão automatizada.

15.2. O titular dos dados poderá se opor ao tratamento com base em uma das hipóteses de dispensa de consentimento, em caso de descumprimento do disposto nestas Cláusulas ou na Legislação Nacional.

15.3. O prazo para resposta às solicitações previstas nesta Cláusula e no item 14.3 é de 15 (quinze) dias a contar da data da solicitação do Titular dos Dados, exceto na hipótese de prazo diferente estabelecido em regulamentação específica da ANPD.

15.4. Caso a solicitação do Titular dos Dados seja dirigida à Parte não designada como responsável pelas obrigações previstas nesta Cláusula ou no item 14.3, a referida Parte deverá:

a) informar ao Titular dos Dados o canal de atendimento disponibilizado pela Parte Designada; ou

b) encaminhar a solicitação à Parte Designada com a maior antecedência possível, de modo a possibilitar a resposta dentro do prazo previsto no item 15.2.

15.5. As Partes informarão imediatamente aos Agentes de Tratamento de Dados com quem tenham compartilhado dados a correção, exclusão, anonimização ou bloqueio dos dados, para que sigam o mesmo procedimento, exceto nos casos em que essa comunicação seja comprovadamente impossível ou envolva um esforço desproporcional.

15.6. As Partes deverão promover a assistência mútua para responder às solicitações dos Titulares dos Dados.

CLÁUSULA 16. Comunicação de Incidente de Segurança

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 Subjects, according to the provisions of National Legislation.

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

16.1. A Parte Designada deverá notificar a ANPD e o Titular dos Dados, em até 3 (três) dias úteis, da ocorrência de um incidente de segurança que possa acarretar risco ou dano relevante aos Titulares dos Dados, de acordo com o disposto na Legislação Nacional.

16.2. O Importador deverá manter um registro dos incidentes de segurança de acordo com a Legislação Nacional.

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:

CLÁUSULA 17. Responsabilidade e indenização por danos

17.1. A Parte que, no exercício das atividades de tratamento de Dados Pessoais, causar dano patrimonial, moral, individual ou coletivo, por violar o disposto nestas Cláusulas e na Legislação Nacional, deverá indenizá-lo.

17.2. O Titular dos Dados poderá pleitear indenização por danos causados por qualquer das Partes em decorrência da violação destas Cláusulas.

17.3. A defesa dos interesses e direitos dos Titulares dos Dados poderá ser pleiteada em juízo, individual ou coletivamente, de acordo com o disposto na legislação pertinente aos instrumentos de proteção individual e coletiva.

17.4. A Parte que atuar como Operador será solidariamente responsável pelos danos causados pelas atividades de tratamento quando deixar de cumprir estas Cláusulas ou quando não tiver seguido as instruções lícitas do Controlador, exceto pelo disposto no item 17.6.

17.5. Os Controladores diretamente envolvidos nas atividades de tratamento que resultaram em danos ao Titular dos Dados serão solidariamente responsáveis por esses danos, exceto pelo disposto no item 17.6.

17.6. As partes não serão responsabilizadas se comprovarem que:

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 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

a) não realizaram o tratamento dos Dados Pessoais atribuídos a elas;
b) embora tenham realizado o tratamento dos Dados Pessoais a elas atribuídos, não houve violação destas Cláusulas ou da Legislação Nacional; ou
c) o dano for decorrente de culpa exclusiva do Titular dos Dados ou de um terceiro que não seja destinatário da Transferência Subsequente ou não seja subcontratado pelas Partes.

17.7. Nos termos da Legislação Nacional, o juiz poderá inverter o ônus da prova em favor do Titular dos Dados sempre que, a seu critério, a alegação for verossímil, não houver provas suficientes ou quando o Titular dos Dados for excessivamente onerado pela produção de provas.

17.8. Os processos judiciais de indenização por danos coletivos que pretendam estabelecer a responsabilidade nos termos desta Cláusula poderão ser conduzidos coletivamente em juízo, observadas as disposições da legislação pertinente.

17.9. A Parte que indenizar o dano ao Titular dos Dados terá direito de regresso contra as demais partes responsáveis, na medida de sua participação no evento danoso.

CLÁUSULA 18. Salvaguardas para Transferências Subsequentes

O Importador somente realizará Transferências de Dados Pessoais sujeitas à Transferência Internacional de Dados regida por estas Cláusulas se expressamente autorizado, de acordo com os termos e condições descritos na CLÁUSULA 3.

18.1. Em qualquer caso, o Importador:

a) deverá se certificar de que a finalidade da Transferência Subsequente é compatível com as finalidades específicas descritas na CLÁUSULA 2;
b) garantirá, por meio de instrumento contratual escrito, que as salvaguardas previstas nestas Cláusulas serão asseguradas pelo terceiro

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.

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,

destinatário da Transferência; e

c) para os fins destas Cláusulas, e com relação aos Dados Pessoais transferidos, será considerado responsável por eventuais irregularidades cometidas pelo terceiro destinatário da Transferência Posterior.

18.2. A Transferência Subsequente também poderá ser realizada com base em outra modalidade válida de Transferência Internacional de Dados prevista na Legislação Nacional, independentemente da autorização de que trata a CLÁUSULA 3.

CLÁUSULA 19. Notificação de Solicitação de Acesso

19.1 O Importador notificará o Exportador e o Titular dos Dados sobre qualquer Solicitação de Acesso relacionada aos Dados Pessoais sujeitos à Transferência Internacional de Dados regida por estas Cláusulas, exceto no caso de a notificação ser proibida pela lei do país em que os dados são tratados.

19.2. O Importador deverá implementar as medidas legais apropriadas, incluindo ações judiciais, para proteger os direitos dos Titulares dos Dados sempre que houver fundamento jurídico adequado para questionar a legalidade da Solicitação de Acesso e, se aplicável, a proibição de emissão da notificação referida no item 19.1.

19.3. Para atender às solicitações da ANPD e do Exportador, o Importador deverá manter um registro das Solicitações de Acesso, incluindo data, solicitante, finalidade da solicitação, tipo de dados solicitados, número de solicitações recebidas e medidas legais implementadas.

CLÁUSULA 20. Rescisão do tratamento e exclusão de dados

20.1. As Partes deverão apagar os dados pessoais sujeitos à Transferência Internacional de Dados regida por estas Cláusulas após o término de seu tratamento, sendo seu armazenamento autorizado apenas para as seguintes finalidades

a) cumprimento de uma obrigação legal ou regulamentar pelo Controlador;

b) estudo por um Órgão de Pesquisa,

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:

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.

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.

garantindo, sempre que possível, a anonimização dos dados pessoais;

c) transferência a terceiros, mediante o cumprimento dos requisitos estabelecidos nestas Cláusulas e na Legislação Nacional; e

d) uso exclusivo do Controlador, sendo vedado o acesso por terceiros, e desde que os dados tenham sido anonimizados.

20.2. Para os fins desta Cláusula, o tratamento dos dados pessoais cessará quando:

a) a finalidade estabelecida nestas Cláusulas tiver sido atingida;

b) Os Dados Pessoais não forem mais necessários ou pertinentes para atingir a finalidade específica pretendida estabelecida nestas Cláusulas;

c) na rescisão do período de tratamento;

d) for atendida a solicitação do Titular dos Dados; e

e) por ordem da ANPD, quando da violação do disposto nestas Cláusulas ou na Legislação Nacional.

CLÁUSULA 21. Segurança do tratamento de dados

21.1. As Partes deverão implementar Medidas de Segurança que garantam proteção suficiente aos Dados Pessoais objeto da Transferência Internacional de Dados regida por estas Cláusulas, mesmo após sua rescisão.

21.2. As Partes informarão, na SEÇÃO III, as Medidas de Segurança implementadas, considerando a natureza das informações tratadas, as características específicas e a finalidade do tratamento, o estado atual da tecnologia e a probabilidade e gravidade dos riscos aos direitos dos Titulares dos Dados, especialmente no caso de dados pessoais sensíveis e de crianças e adolescentes.

21.3. As Partes envidarão os esforços necessários para implementar medidas de avaliação e revisão periódicas para manter o nível adequado de segurança de dados.

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.

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

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.

CLÁUSULA 22. Legislação do país de destino

22.1 O Importador declara que não identificou quaisquer leis ou práticas administrativas do país destinatário dos Dados Pessoais que o impeçam de cumprir as obrigações assumidas nestas Cláusulas.

22.2. Na hipótese de mudança regulatória que altere essa situação, o Importador deverá notificar imediatamente o Exportador para avaliar a continuidade do contrato.

CLÁUSULA 23. Descumprimento das Cláusulas pelo Importador

23.1. Na hipótese de descumprimento das salvaguardas e garantias previstas nestas Cláusulas ou estando o Importador impossibilitado de cumprir qualquer uma delas, o Exportador será imediatamente notificado, observado o disposto no item 19.1.

23.2. Recebida a comunicação a que se refere o item 23.1 ou verificado o descumprimento destas Cláusulas pelo Importador, o Exportador implementará as medidas pertinentes para assegurar a proteção dos direitos dos Titulares dos Dados e a conformidade da Transferência Internacional de Dados com a Legislação Nacional e com estas Cláusulas, podendo, conforme o caso:

a) suspender a Transferência Internacional de Dados;
b) solicitar a devolução dos Dados Pessoais, sua transferência para um terceiro ou sua exclusão; e
c) rescindir o contrato.

CLÁUSULA 24. Escolha de foro e jurisdição

24.1. A legislação brasileira se aplica a estas Cláusulas e qualquer controvérsia entre as Partes decorrente destas Cláusulas deverá ser resolvida perante os tribunais competentes no Brasil, observando, se aplicável, o foro escolhido pelas Partes na Seção IV.

24.2. Os Titulares dos Dados poderão ajuizar ações judiciais contra o Exportador ou o Importador, conforme sua escolha, perante os tribunais competentes no Brasil, inclusive aqueles de seu local de residência.

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.

24.3. De comum acordo, as Partes poderão se valer da arbitragem para resolver conflitos decorrentes destas Cláusulas, desde que o procedimento seja realizado no Brasil e de acordo com as disposições da Lei de Arbitragem.

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).

SEÇÃO III - Medidas de Segurança

(OBSERVAÇÃO: Essa Seção deve incluir detalhes das medidas de segurança implementadas, incluindo medidas específicas para a proteção de dados confidenciais e de crianças e adolescentes. As medidas podem incluir os seguintes aspectos, entre outros, conforme indicado na tabela abaixo).

(i) governance and supervision of internal processes: (ii) technical and administrative security measures, including measures to guarantee the security of the operations carried out, such as the collection, transmission and storage of data:

(i) governança e supervisão de processos internos: (ii) medidas de segurança técnicas e administrativas, incluindo medidas para garantir a segurança das operações realizadas, como a coleta, a transmissão e o armazenamento de dados:

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).

SEÇÃO IV - Cláusulas Adicionais e Anexos

(OBSERVAÇÃO: Nesta Seção, de preenchimento e divulgação facultativos, poderão ser incluídas, a critério das Partes Divulgadoras, Cláusulas Adicionais e Anexos para regular, entre outras, questões de natureza comercial, rescisão contratual, prazo de vigência e eleição de foro no Brasil. Conforme previsto no Regulamento Internacional de Transferência de Dados, as cláusulas estabelecidas nesta Cláusula ou em Contratos Relacionados não poderão excluir, modificar ou contrariar, direta ou indiretamente, as Cláusulas previstas nas Seções I, II e III).