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

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

1. **Definitions.** For the purposes of this Addendum, the following terms shall have the following meanings:
   a. **Affiliate(s)**: means any other legal entity that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such entity. The term "control" (including the terms "controlled by" and "under common control with") means the direct or indirect power to direct or cause the direction of the management and policies of an entity, whether through the ownership of voting securities, by contract, or otherwise of more than fifty percent (50%) of the voting securities of an entity.
   b. **"Data Privacy Laws"** means any laws that apply to the Processing of Personal Data by Supplier under the Primary Agreement. This includes laws, regulations, guidelines, requirements, and government issued rules in the U.S. and other jurisdictions, at the international, national, state/provincial, or local levels, currently in effect and as they become effective, including without limitation EU Directive 95/46/EC, the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), the UK Data Protection Act, 2018, the California Consumer Privacy Act of 2018 ("CCPA") as amended by the California Privacy Rights Act of 2020 ("CPRA"), the Virginia Consumer Data Protection Act ("VCDPA"), the Colorado Privacy Act ("CPA"), the New York SHIELD Act, the Federal Law for the Protection of Personal Data held by Private Parties and its regulations ("FDPL"), the Brazilian Data Protection Law No. 13,709/2018 (the "LGPD"), and any applicable data security and/or privacy laws of other jurisdictions as may be amended from time to time.
   c. **"Data Subject"** means the individual to whom Personal Data relates.
   d. "**Information System**" means computer, communication, and network equipment, systems, and services (voice, data, or otherwise) owned, controlled, or used by CHS, including, but not limited to, the corporate wide area network, the electronic switched network, Inter/intranet gateways, electronic mail, telephony, computer systems, system hardware, drives, electronic media, storage areas, software programs, files, and databases.
   e. **"Permitted System"** means a CHS Information System to which CHS or CHS Affiliates expressly grants Supplier access and that is necessary for Supplier to perform its obligations to the CHS.
   f. **"Personal Data"** means any information received by the Supplier from CHS, or on the CHS's behalf, that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household.
   g. **"Process" or "Processing"** means any operation or set of operations that is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
   h. "**Security Incident**" means any unlawful or unauthorized access to any of CHS's Personal Data stored on Supplier's equipment or in Supplier's facilities, or access to equipment or facilities resulting in any unauthorized use, acquisition, Processing, loss, destruction, damage, disclosure, theft, copying, modification, or alteration of CHS Personal Data.

2. Obligations of the Supplier.

The Supplier represents and warrants that:

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

b. It will notify CHS in writing, which includes notice to privacy@chsinc.com, immediately upon making a determination that it has not met, or can no longer meet, its obligations under Section 2(a) of this Addendum. In such case, Supplier will abide by CHS's written instructions, including instructions to cease further Processing of the Personal Data, and shall take any necessary steps to remediate any Processing of such Personal Data not in accordance with Section 2(a) of this Addendum.

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

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

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

Data, as well as providing CHS with a list of Personal Data elements about a specific individual held by Supplier on CHS's behalf, upon CHS's request and within 15 days of receiving such request.

f. Promptly, but within no later than forty-eight (48) hours, notify CHS if it receives a request for subject access, rectification, cancellation, objection, restriction, data portability, or revocation of consent for the Processing of Personal Data, or any other data protection related requests. Supplier shall not respond to such requests directly, unless expressly authorized by the CHS in writing. Should any court, government agency or law enforcement agency contact Supplier with a demand for CHS's Data, Supplier will direct the law enforcement agency to request such information directly from CHS. As part of this effort, Supplier may provide CHS's basic contact information to the agency. If compelled to disclose CHS's Data to law enforcement, then Supplier will promptly, and without any undue delay, notify CHS and deliver a copy of the request (except where Supplier is legally prohibited from doing so) to allow CHS to seek a protective order or any other appropriate remedy. To the extent permitted by applicable law, Supplier shall take all reasonable actions to prevent disclosure of CHS Personal Data to a government agency and/or in response to a legal demand such as subpoena or similar demand, without CHS's prior express written consent. If and only to the extent that is not legally possible, Supplier will notify CHS in advance of any disclosure and provide CHS with the opportunity to object, unless prohibited by applicable law.

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.*

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

4. **Security Incident.** Supplier shall notify CHS immediately, and no later than 48 hours after discovery, in writing in the event that: (i) any Personal Data is disclosed or is suspected to have been disclosed by Supplier in violation of the Primary Agreement and/or this Addendum, or applicable Data Privacy Laws or (ii) Supplier discovers, is notified of, or suspects that a Security Incident involving Personal Data has occurred, may have occurred, or may occur.
    a. If the Primary Agreement provides for a specific CHS contact, Supplier will notify that contact and also send an e-mail notification to CHSinformationsecurity@chsinc.com. If the agreement or other terms and conditions under which Supplier provides goods, services, or software to the CHS do not provide for a specific contact, Supplier will notify CHS Information Security by e-mail at CHSinformationsecurity@chsinc.com and/or IT Service Center Phone: 651-355-5555 or 800-852-8185. Supplier will also provide to CHS any other notice required by law.
    b. Supplier shall cooperate fully in the investigation of the Security Incident, indemnify and reimburse CHS for any and all damages, losses, fees, fines or costs (whether direct, indirect, special or consequential), including reasonable attorneys' fees and costs, incurred as a result of such incident, and remedy any harm or potential harm caused by such incident. To the extent that a Security Incident gives rise to a need, in CHS's sole judgment to provide (i) notification to public authorities, individuals, or other persons, or (ii) undertake other remedial measures (including, without limitation, notice, credit monitoring services and the establishment of a call center to respond to inquiries (each of the foregoing a "Remedial Action(s)")), at CHS's request, Supplier shall, at Supplier's cost,

undertake such Remedial Actions. The timing, content and manner of effectuating any notices shall be determined by CHS in its sole discretion.

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

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

5. Cross-Border Transfer of Personal Data. Supplier shall not Process Personal Data in a jurisdiction outside of the agreed Processing location without the written consent of CHS. To the extent that Personal Data includes information about individuals who are located in the European Economic Area ("EEA"), the UK, Argentina or Switzerland, and Supplier or any subcontractors store or otherwise obtain access to such Personal Data outside of the EEA, UK, Argentina or Switzerland, the Supplier agrees to Process this Personal Data in accordance with the EU Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to the Commission Implementing Decision (EU) 2021/914, Module Two, which is incorporated by reference herein ("Model Processor Contract" or "SCC"), the UK International Data Transfer Addendum ("UK Addendum"), which are incorporated here by reference, for Personal Data on which the UK data protection laws apply, and for Personal Data on which the Swiss or Argentine data protection laws apply including the specific Swiss or Argentine local law amendments to the Model Processor Contract. To the extent that Personal Data includes information about individuals who are located in Brazil, and were located in Brazil at the moment that the information was collected and Supplier or any subcontractors store or otherwise obtain access to such Personal Data outside of Brazil, the Supplier agrees to Process this Personal Data in accordance with the Brazilian Model Clauses ("BMC"), as published by the Brazilian Data Protection Authority ("ANPD"), which are incorporated here as Annex II. To the extent that Supplier Processes Personal Data in a particular jurisdiction other than the EEA, UK, Argentina or Switzerland, and such Processing would be prohibited by applicable privacy laws in the absence of the implementation of terms comparable to the Model Processor Contract, Supplier shall Process all such Personal Data in accordance with the Model Processor Contract, and for such purposes, references to EU/EEA jurisdictions shall be deemed to be references to the relevant non-EU/EEA jurisdictions as applicable.

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

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

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

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

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

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

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

6. Miscellaneous Obligations.

- **a.** Supplier shall, upon the CHS's request, promptly execute supplemental data processing agreement(s) with CHS or any of its subsidiaries, provide necessary assistance or take other appropriate steps, to its best efforts, to address cross-border transfer and other requirements if CHS concludes, in its sole judgment, that such supplemental data processing agreement(s), assistances, and steps are necessary to address applicable Data Privacy Laws concerning Personal Data.
- **b.** Supplier will appoint a data protection officer where such appointment is required by data protection laws. The appointed person may be reached by email via the email address provided by Supplier on the signature page of this DPA. Supplier will promptly notify CHS of any change in the data protection officer contact information.
- **c.** Supplier certifies that it understands and will comply, and cause all Supplier personnel to certify that they understand and will comply with the requirements of this Addendum.
- **d.** The parties agree that, to the extent such right is clearly established in the Primary Agreement, Supplier may use CHS's Personal Data on the CHS's behalf. In such cases, CHS instructs Supplier to use only de-identified or aggregate information, and, for the sake of clarity, CHS instructs Supplier to first anonymize, aggregate, and/or de-identify the Personal Data as necessary for that purpose. With respect to such de-identified or aggregated information: (1) Supplier shall comply with all applicable laws, including the implementation of: (a) technical safeguards that prohibit reidentification; (b) business processes that specifically prohibit reidentification; (c) business processes to prevent inadvertent release of deidentified information; and (2) Supplier shall make no attempt to reidentify the information.
- **e.** At all times at which Supplier holds CHS's Personal Data, Supplier will have in place a bona fide business continuity plan that will ensure that Supplier is able to continue to provide services when the

provision of such services is interrupted for any reason outside of Supplier's reasonable control ("Business Continuity Plan"). Supplier shall maintain and update the Business Continuity Plan at least annually for each of its operational sites related to the provision of services. Supplier will put the Business Continuity Plan in effect if a site becomes unable to perform such services or deliver services for a period of more than five (5) calendar days. Supplier will perform a timely assessment after the occurrence of any event that may delay the performance of maintenance and support or the delivery of services for a period of more than five (5) calendar days. Supplier will activate the Business Continuity Plan if Supplier determines that Supplier will be unable to perform services for a period of more than five (5) calendar days.

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.
   - **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

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

Supplier

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

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

Signed by:
[Insert Supplier name]

_____
Signature

_____
Name

_____
Date

_____
Title

Email Address of DPO, if applicable

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].*

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.

ANNEX I - INFORMATION SECURITY REQUIREMENTS

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

1. Information Security.

a. Supplier will implement and maintain a written information security program including appropriate policies, procedures, and risk assessments that are reviewed at least annually.

b. Supplier will implement administrative, physical, and technical safeguards to:

   i. Protect CHS Personal Data from unauthorized access, exfiltration, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage;

   ii. Supplier will not utilize or store any CHS Personal Data in self-improving or machine learning software, models, algorithms, hardware or other tools or aids of any kind, and

   iii. Take all necessary steps in mitigating damage, losses, costs and expenses caused by the events set forth in Section 4 of this Addendum.

c. Supplier shall notify CHS of any significant changes to administrative, physical, or technical safeguards, that could reasonably be expected to adversely affect the protection of CHS Personal Data from unauthorized access, exfiltration, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage.

d. All right, title and interest in CHS Personal Data will remain the property of CHS. Supplier has no intellectual property rights or other claim to CHS Personal Data that is hosted, stored, or transferred to and from Supplier's own systems and facilities or a third party hosted cloud provider. CHS Personal Data will not be used for analytics, marketing or anything outside of the intended use set out in this Agreement, or for the benefit of anyone other than CHS.

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

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

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

   ii. Inventory of Authorized and Unauthorized Software. Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and ensure that unauthorized and unmanaged software is found and prevented from installation or execution.

   iii. Secure Configuration of Enterprise Assets and Software. Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile;

network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

c. Suppliers will, upon CHS's request, make available to CHS for review, as applicable, Supplier's latest Payment Card Industry ("PCI") Compliance Report, SOC audit report, or any industry standard independent audit reports or certifications performed by or on behalf of Supplier assessing the effectiveness of Supplier's information security program as relevant to the CHS Personal Data.
    i. SOX: If Supplier is in scope for CHS's compliance with the Sarbanes–Oxley Act (the "SOX Act"), as may be amended from time to time, Supplier will provide annually to CHS, for review, Supplier's latest SOC report for as long as the system holds, contains or Processes CHS Personal Data, or
    ii. PCI: Supplier will provide annually to CHS, for review, Supplier's latest PCI Compliance Report(s) and/or SOC report for as long as the system holds, contains or Processes CHS Personal Data.

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

providers to attest to the results of a PCI DSS assessment.;

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

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

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

v. Provide to CHS an agreed upon responsibility matrix identifying which PCI DSS requirements will be managed by the Supplier; and

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

3. Access to CHS Information Systems

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

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

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

d. Specific Prohibitions. Except as expressly authorized by CHS in a signed writing (whether in a statement of work, project specification, work order, or separate written direction) Supplier shall not (i) attempt to reverse engineer, disassemble, reverse translate, decompile, or in any other manner decode any element of the CHS Information Systems; (ii) attempt to decrypt encrypted or scrambled information; (iii) make modifications, enhancements, adaptations or translations, in whole or in part, to or of any element of the CHS Information Systems, not authorized by CHS; (iv) access any CHS Information System in excess of the permission expressly granted by the CHS; (v) make copies of any element of the CHS Information Systems; (vi) use any CHS Information System or data to build a competitive product or service, or otherwise for commercial purposes; (vii) probe host computers or networks; (viii) breach or examine the security controls of a host computer, network component or authentication system, or circumvent or disclose CHS Information System user authentication or security controls; (ix) monitor data on any network or system without CHS's written authorization; (x) interfere with or disrupt the service of any user, host or network, or overload a server, network connected device, or network component or otherwise threaten harm to property; (xi) originate malformed data or network traffic that results in damage to, or disruption of, a service or network connected device; (xii) forge data or misrepresent the origination of a user or source; (xiii) take any action that is unlawful, abusive, malicious, harassing, tortious, defamatory, libelous or invasive of another's privacy right or infringing the IP rights of any person; (xiv) otherwise violate any applicable law or regulation;

(xv) permit access by a competitor of CHS. Should an authorized Supplier personnel take any action in violation of this section, CHS may require Supplier to replace the authorized Supplier personnel with another authorized Supplier personnel or suspend or terminate the Primary Agreement, statement of work, or order in its sole discretion, while preserving any other remedy available to CHS.

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

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

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

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

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

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 International Data Transfer governed by these Clauses, except in the cases provided for in item 18.3.

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

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

CLAUSE 4. Responsibilities of the Parties

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

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

( ) Exporter ( ) Importer

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

( ) Exporter ( ) Importer

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

( ) Exporter ( ) Importer

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

a) compliance with the obligations provided in CLAUSES 14, 15 and 16 and other provisions established in the National Legislation, especially in case of omission or non-compliance with the obligations by the Designated Party;

b) compliance with ANPD's determinations; and

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

SECTION II – MANDATORY CLAUSES

CLAUSE 5 Purpose

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

CLAUSE 6. Definitions

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

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

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.

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;
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.

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.

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 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.

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.

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, consumer and credit profile or aspects of their personality; and
k) information on the criteria and procedures adopted for the automated decision.

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

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

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

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

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

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

CLAUSE 16. Security Incident Reporting

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

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

CLAUSE 17. Liability and compensation for damages

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

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

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

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

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

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

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

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

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

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

CLAUSE 18. Safeguards for Onward Transfers

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

18.1. In any case, the Importer:

a) shall ensure that the purpose of the Onward Transfer is compatible with the specific purposes described in CLAUSE 2;
b) shall guarantee, by means of a written contractual instrument, that the safeguards provided in these Clauses shall

be ensured by the third-party recipient of the Onward Transfer; and

c) for the purposes of these Clauses, and regarding the Personal Data transferred, shall be considered responsible for any eventual irregularities committed by the third-party recipient of the Onward Transfer.

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

CLAUSE 19. Access Request Notification

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

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

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

CLAUSE 20. Termination of processing and erasure of data

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

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

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

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.

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.

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

SECTION III - Security Measures

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

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

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).